

**DISEÑO DE UN MODELO DE GESTIÓN PARA LA COMUNICACIÓN
CORPORATIVA ENTRE SEDES DE AUTOBOL S.A. APOYADO EN T.I.**

**MARCELA PATRICIA MEZA ALMEIDA
ELIAS AHUMEDO ZAMORA
VICKMATOR OTON ANAYA BARRERA
JOSE ALEJANDRO LLORENTE DORIA**

**ESPECIALIZACIÓN EN GERENCIA DE SISTEMAS DE INFORMACIÓN
UNIVERSIDAD DEL NORTE
CARTAGENA
2007**

**DISEÑO DE UN MODELO DE GESTIÓN PARA LA COMUNICACIÓN
CORPORATIVA ENTRE SEDES DE AUTOBOL S.A. APOYADO EN T.I.**

**MARCELA PATRICIA MEZA ALMEIDA
ELIAS AHUMEDO ZAMORA
VICKMATOR OTON ANAYA BARRERA
JOSE ALEJANDRO LLORENTE DORIA**

**Trabajo Integrador para optar al título de postgrado de Especialista en
Gerencia de Sistemas de Información**

**Coautor:
Jorge Alberto Gil Peñaloza**

**ESPECIALIZACIÓN EN GERENCIA DE SISTEMAS DE INFORMACIÓN
UNIVERSIDAD DEL NORTE
CARTAGENA
2007**

AGRADECIMIENTOS

Los autores expresan su agradecimiento a:

Jorge Alberto Gil Peñaloza, por su oportuna y muy decidida colaboración, la que permitió el desarrollo de este trabajo y el cumplimiento de sus objetivos.

Luz Stella Robles Pedrozo, por su labor y compromiso mostrado con el grupo de la especialización.

A todos los profesores de la especialización, por compartir sus experiencias y conocimientos.

ÍNDICE

1. OBJETIVO GENERAL	9
2. OBJETIVOS ESPECÍFICOS	9
3. JUSTIFICACIÓN	10
4. MARCO TEÓRICO	10
4.1. Introducción	10
4.2. Contenido.....	11
4.2.1. MSV[1]	12
4.2.2. COSO [4][5].....	14
4.2.2.1. ¿Qué es control interno?.....	15
4.2.2.2. Los cinco componentes del control interno	15
4.2.3. Planeación Estratégica	28
4.2.3.1. Misión.....	28
4.2.3.2. Visión	29
4.2.3.3. Valores.....	29
4.2.3.4. Cadena de Valor	29
5. MODELO PROPUESTO.....	31
5.1. Análisis Interno Actual de la Organización.....	32
5.1.1. Entradas.....	32
5.1.2. Metodología	33
5.1.3. Salidas	33
5.2. Generación de Mecanismos de Control de la Comunicación.....	33
5.2.1. Entradas.....	33
5.2.2. Metodología	33
5.2.3. Salidas	34
5.3. Diseño de Mecanismo de Seguridad de T.I.....	34
5.3.1. Entradas.....	34
5.3.2. Metodología	34
5.3.3. Salidas	35
6. IMPLEMENTACIÓN DEL MODELO PROPUESTO EN UNA SITUACIÓN REAL	36
6.1. Etapa 1 - Análisis Interno Actual de la Organización	36
6.1.1. Entradas.....	36
6.1.1.1. Antecedentes.....	36
6.1.1.2. Misión de Autobol S.A.....	38

6.1.1.3.	Visión de Autobol S.A.....	39
6.1.1.4.	Valores de Autobol S.A.....	39
6.1.1.5.	Cadena de Valor Autobol S.A.	40
6.1.1.6.	Proceso de Recepción de Vehículos Nuevos	40
6.1.1.7.	Proceso De Alistamiento De Vehículos Nuevos	43
6.1.1.8.	Proceso De Entrega De Vehículos Nuevo	46
6.1.1.9.	Proceso De Venta De Repuestos Para Vehículos Mazda	50
6.1.1.10.	Proceso En La Estación De Servicios.....	51
6.1.1.11.	Situación Actual Del Entorno Informático	51
6.1.2.	Metodología	54
6.1.3.	Salidas	54
6.1.3.1.	Matriz de Riesgos	54
6.1.3.2.	Necesidades del área de T.I.	56
6.2.	Etapa 2 – Generación de Mecanismos de Control de la Comunicación.....	56
6.2.1.	Entradas.....	56
6.2.2.	Metodología	57
6.2.3.	Salidas	57
6.2.3.2.	Situación Propuesta Del Entorno Informático	59
6.2.3.3.	Políticas de sistemas	66
6.2.3.4.	Política de seguridad y control informático.....	66
7.	CONCLUSIONES.....	73
8.	BIBLIOGRAFÍA.....	74

ANEXOS

ÍNDICE DE GRÁFICOS

Gráfico 1. MSV.....	14
Gráfico 2. Modelo Propuesto.....	31
Gráfico 3. Cadena de valor.....	40
Gráfico 4. Proceso de Recepción de Vehículos nuevos.....	41
Gráfico 5. Proceso de Alistamiento de Vehículos Nuevos.....	44
Gráfico 6. Proceso de Entrega de Vehículos nuevos.....	47

ÍNDICE DE TABLAS

Tabla 1. Matriz de Riesgos.....55

LISTA DE ANEXOS

ANEXO A: Red Autobol Actual

ANEXO B: Red Propuesta Cartagena

ANEXO C: Red Propuesta Valledupar

ANEXO D: Hoja de Datos [3COM® OfficeConnect® VPN Firewall](#)

TÍTULO

Diseño de un modelo de gestión para la comunicación corporativa entre sedes de Autobol S.A. apoyado en T.I.

1. OBJETIVO GENERAL

Realizar el diseño de un modelo de gestión para la comunicación entre las sedes de Autobol S.A. apoyados en T.I.

2. OBJETIVOS ESPECÍFICOS

Proponer un modelo que cuente con las siguientes fases:

- Diseñar estrategias que permitan administrar y controlar el uso de los recursos informáticos entre las sedes de Autobol S.A.
- Hacer uso del Modelo del Sistema Viable (MSV de sus siglas en inglés Viable System Model) [1] para generar un modelo de comunicación que sea sostenible en el tiempo.
- Proponer políticas de control y seguridad informática que garanticen la autenticidad y la confiabilidad de las comunicaciones entre las sedes.
- Emplear dicho modelo para implementar algunas de sus fases en una situación real, dentro del tiempo asignado al desarrollo de este trabajo, como requisito dentro del programa de especialización.

3. JUSTIFICACIÓN

Consideramos que todos los procesos que son parte de las organizaciones deben ser revisados periódicamente, no solo con el fin de ejercer labores de supervisión y monitoreo sino también buscando acciones de mejoras continuas o permanentes que se puedan aplicar para contribuir con la supervivencia de las mismas. En estos tiempos de globalización y competitividad los negocios tienen que ser como seres vivientes que se puedan adaptar fácilmente y sobrevivir a los cambios vertiginosos para no sucumbir en un mundo que se transforma rápidamente y que da cuenta de quienes no logran estar pensando a futuro.

De igual forma opinamos que el cambio en las organizaciones se debe dar haciendo la comparación de lo interior con lo exterior, analizando el entorno, actualizando sus procesos a las mejores prácticas del sector en que se mueven y realizando seguimiento al cumplimiento de los objetivos del negocio.

El modelo de gestión que proponemos se basa en el MSV y en los cinco componentes del control interno, ya que en estos podemos encontrar como realizar un análisis profundo a la organización, en donde se tienen en cuenta los aspectos propios de la misma, que la identifican como tal, que permiten la adaptación de la organización ante posibles cambios y la regulación o monitoreo de sus procesos.

4. MARCO TEÓRICO

4.1. Introducción

De acuerdo con la experiencia de los autores de este trabajo, se considera que son muchos los modelos, las herramientas y metodologías que los profesionales

pueden aplicar para todas las actividades que conciernen a la gestión de la tecnología informática y la ingeniería de sistemas, las cuales abarcan bastantes tópicos que al estar bien definidos y controlados pueden aumentar la probabilidad de llevar a los negocios al éxito, entre estos podemos encontrar: la administración de redes informáticas y de las telecomunicaciones, el análisis de procesos, la gestión y control de tecnología informática, la administración de portafolio de proyectos, la planeación estratégica de T.I., gerencia y la evaluación financiera de proyectos.

Estos modelos, herramientas y metodologías hacen parte fundamental de la Especialización de Gerencia de Sistemas de Información de la Universidad del Norte y se tuvieron presentes, se mencionan y se utilizan para el desarrollo de este trabajo integrador, según se fue requiriendo de acuerdo con el contenido tratado en este.

Como base para el desarrollo de este trabajo integrador se utilizó, primordialmente y entre otros, el MSV [1] y se aplicaron sus fundamentos para diseñar el modelo que se pretende proponer. Más adelante se explicará el porque de la escogencia del MSV [1] y de otros modelos, pero en menor intensidad, para el desarrollo de los objetivos de este trabajo.

En concepto de sus autores, esta metodología no solo servirá de apoyo a Autobol S.A. para realizar su gestión de comunicación entre sus sedes, sino también a otras empresas similares en el negocio o en el tamaño de su infraestructura.

4.2. Contenido

El marco teórico de este trabajo está relacionado con:

- Modelo del Sistema Viable (MSV) [1]

- COSO y los cinco componentes del control interno
 - Ambiente de Control
 - Evaluación de Riesgos
 - Actividades de Control
 - Información y Comunicación
 - Supervisión o Monitoreo.
- Planeación Estratégica [2]
 - Misión
 - Visión
 - Valores
 - Cadena de Valor

4.2.1. MSV[1]

Hoy en día, las organizaciones están obligadas a adaptarse a los cambios constantes que se presentan en su entorno, para esto es necesario hacer uso de una herramienta que permita estudiar la situación actual de la organización, identificar las problemáticas, generar posibles soluciones y realizar un monitoreo constante a los procesos internos, como también evaluar las estrategias en función de la complejidad de las tareas que se realizan en el interior de la organización.

En consideración de los autores de este estudio, una herramienta posible es la conocida como el MSV [1] desarrollada por el científico inglés Stafford Beer.

El MSV [1] es el más representativo y de mayor uso de la cibernética. Sus principales conceptos son la comunicación, la información, la retroalimentación, y los principios deducidos de la observación de los homomorfismos entre el

comportamiento de sistemas físicos y sociales. Posee las siguientes ventajas en comparación a otros modelos existentes:

- No requiere la existencia previa de la organización en estudio.
- Es una herramienta de complejidad.
- Rompe el esquema jerárquico de entenderse dentro de la organización.
- Involucra la realización de identidad organizacional.
- Realiza una sinapsis entre los elementos internos y externos de la organización (adaptación), usando como referencia la Ley de la Variedad Requerida, que en forma general establece que, un controlador tiene un requisito de variedad, si y solo si, tiene la capacidad para mantenerse dentro de un conjunto de objetivos deseados.

Las cinco funciones esenciales que deben funcionar con eficacia en una organización para que haya viabilidad son:

Subsistema Uno: Función de Implementación, es la identidad e la organización.

Subsistema Dos: Función de Coordinación, esta identificado por una función de regulación, que mantiene en equilibrio la función Uno.

Subsistema Tres: Función de Control, es la dirección operacional y se preocupa de incorporar a los objetivos globales de la organización a los sistemas uno y es responsable de la conducta de las actividades cotidianas de la corporación.

Subsistema Cuatro: Función de Inteligencia, es la dirección de desarrollo y se preocupa de lo que ocurre afuera de la organización considerando el futuro.

Subsistema Cinco: Función Política, es la dirección corporativa y es lógicamente el que encabeza el eje vertical de mando y por lo tanto el que define las políticas y orientaciones generales de la organización. [3]

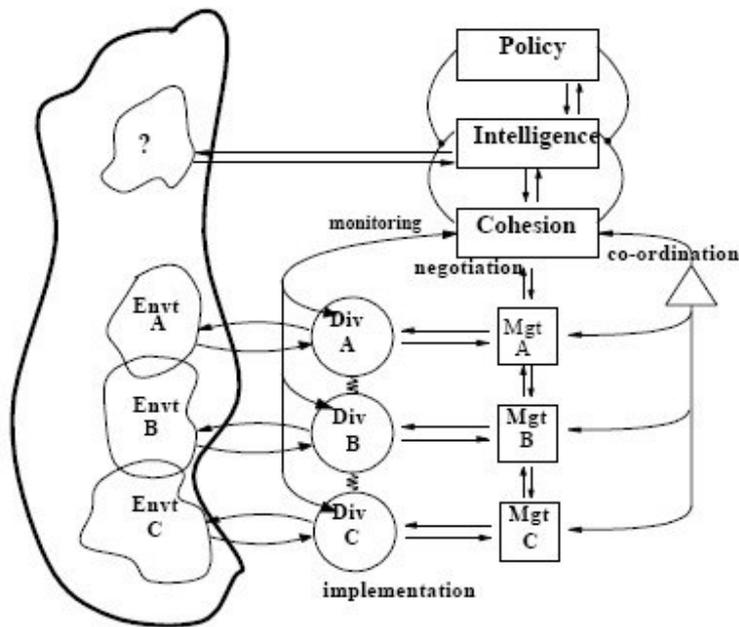


Gráfico 1. MSV [1]

4.2.2. COSO [4][5]

COSO fue originalmente creado en 1985 para patrocinar a la Comisión Nacional sobre el Reporte Fraudulento en Finanzas, fue una iniciativa del sector privado independiente que estudió los factores causales que podían liderar el reporte fraudulento en finanzas y se desarrollaron recomendaciones para compañías públicas y sus auditores independientes o externos, para la Comisión de Seguridad e Intercambio (SEC) y otros entes reguladores y para instituciones educativas.

El objetivo de COSO fue: definir un nuevo marco conceptual del control interno, capaz de integrar las diversas definiciones y conceptos que venían siendo utilizados sobre este tema, logrando así que, al nivel de las organizaciones públicas o privadas, de la auditoría interna o externa, o de los niveles académicos

o legislativos, se cuente con un marco conceptual común, una visión integradora que satisfaga las demandas generalizadas de todos los sectores involucrados.

4.2.2.1. ¿Qué es control interno?

El Control Interno se define como el conjunto de principios, fundamentos, reglas, acciones, mecanismos, instrumentos y procedimientos que ordenados, relacionados entre sí y unidos a las personas que conforman una organización, se constituye en un medio para lograr el cumplimiento de su función administrativa, sus objetivos y la finalidad que persigue, generándole capacidad de respuesta ante los diferentes públicos o grupos de interés que debe atender. [6]

De acuerdo a lo anterior se puede decir que todas las normas que giran al entorno de una organización tienen como finalidad que estas permanezcan en el tiempo siendo productivas y manteniendo niveles aceptables de competitividad, logrando que se puedan posicionar en un mercado objetivo o determinado.

4.2.2.2. Los cinco componentes del control interno

De acuerdo al marco COSO el control interno consta de cinco componentes relacionados entre sí.

Estos derivarán de la manera en que la dirección dirija la unidad y estarán integrados en el proceso de la dirección. Los componentes serán los mismos para todas las organizaciones ya sean públicas o privadas y dependerá del tamaño de la misma la implantación de cada uno de ellos. [7]

a) Ambiente de Control.

El entorno de control marca la pauta del funcionamiento de una empresa e influye en la concienciación de sus empleados respecto al control. Es la base de todos los demás componentes del control interno, aportando disciplina y estructura. Los factores del entorno de control incluyen la integridad, los valores éticos y la capacidad de los empleados de la empresa, la filosofía de dirección y el estilo de gestión, la manera en que la dirección asigna autoridad y las responsabilidades y organiza y desarrolla profesionalmente a sus empleados y la atención y orientación que proporciona al consejo de administración. [8]

FACTORES DEL ENTORNO DE CONTROL (COMO EVALUAR EL ENTORNO DE CONTROL)

Para evaluar el entorno de control, el evaluador debe considerar cada factor del ambiente de control a la hora de determinar si éste es positivo. Algunos aspectos son altamente subjetivos y obligan a que se formule una opinión subjetiva, generalmente inciden de forma significativa en la eficacia del ambiente de control.

INTEGRIDAD Y VALORES ÉTICOS.

- La existencia e implantación de códigos de conducta u otras políticas relacionadas con las prácticas profesionales aceptables, incompatibilidades o pautas esperadas de comportamiento ético y moral.
- La forma en que se llevan a cabo las negociaciones con empleados, proveedores, clientes, inversionistas, acreedores, competidores y auditores.
- La presión por alcanzar objetivos de rendimiento poco realistas.

COMPROMISO DE COMPETENCIA PROFESIONAL.

- La existencia de descripciones de puestos de trabajo formales.
- El análisis de conocimientos y habilidades para llevar a cabo el trabajo adecuadamente.

CONSEJO DE ADMINISTRACIÓN O COMITÉ DE AUDITORÍA.

- El ambiente de control y la cultura de la organización están influidos de forma significativa por el Consejo de Administración y el Comité de Auditoría, el grado de independencia del Consejo o del Comité de Auditoría respecto de la dirección, la experiencia y la calidad de sus miembros, grado de implicación y vigilancia y el acierto de sus acciones son factores que inciden en la eficacia del Control Interno.
- La independencia de los consejeros o miembros del Comité.
- La frecuencia y oportunidad de las reuniones con el director financiero y/o contable, auditores internos y externos.
- La suficiencia y oportunidad con que se facilita información a los miembros del Consejo o Comité de Auditoría para permitir supervisar los objetivos y las estrategias, la situación financiera, así como los resultados de explotación de la entidad.

SITUACIONES QUE PUEDEN INCITAR A LOS EMPLEADOS A COMETER ACTOS INDEBIDOS.

- Falta de controles o controles ineficaces.

- Alto nivel de descentralización sin las políticas de apoyo necesarias, que impide que la dirección esté al corriente de las acciones llevadas a cabo en los niveles mas bajos.
- Una función de auditoría interna débil.
- Consejo de Administración poco eficaz.
- Sanciones por comportamiento indebido insignificantes o que no se hacen públicas. [9]

El entorno o ambiente de control entonces también ayuda a crear el sentido de pertenencia hacia la empresa e identifica a sus empleados delante de su medio organizacional y los ayuda a su desarrollo profesional y personal.

b) Evaluación de Riesgos.

Las organizaciones, cualquiera sea su tamaño, se enfrentan a diversos riesgos de origen externos e internos que tienen que ser evaluados. Una condición previa a la evaluación del riesgo es la identificación de los objetivos a los distintos niveles, vinculados entre sí e internamente coherentes. La evaluación de los riesgos consiste en la identificación y el análisis de los riesgos relevantes para la consecución de los objetivos, y sirve de base para determinar cómo han de ser gestionados los riesgos. Debido a que las condiciones económicas, industriales, legislativas y operativas continuarán cambiando continuamente, es necesario disponer de mecanismos para identificar y afrontar los riesgos asociados con el cambio. [8]

A nivel de empresa los riesgos pueden ser la consecuencia de factores externos como internos, se presentan algunos ejemplos:

Factores externos:

- Los avances tecnológicos.
- Las necesidades o expectativas cambiantes de los clientes pueden influir en el desarrollo de productos, el proceso de producción, el servicio a cliente, la fijación de precios etc.
- Los cambios económicos pueden repercutir en las decisiones sobre financiamiento, inversiones y desarrollo.

Factores internos:

- Problemas con los sistemas informáticos pueden perjudicar las operaciones de la entidad.
- Los cambios de responsabilidades de los directivos pueden afectar la forma de realizar determinados controles.
- Un Consejo de Administración o un Comité de Auditoría débil o ineficaz pueden dar lugar a que se produzcan fugas de información.

Análisis de riesgos

Una vez identificados los riesgos a nivel de entidad y por actividad deben llevarse a cabo un análisis de riesgos que puede ser:

- Una estimación de la importancia del riesgo.
- Una evaluación de la probabilidad o frecuencia de que se materialice el riesgo.
- Que medidas deben adoptarse.

Las actividades de control pueden dividirse en tres categorías, según el tipo de objetivo de la entidad con el que están relacionadas: las operacionales, la confiabilidad de la información financiera y el cumplimiento de la legislación aplicable. [9]

En la evaluación de riesgos se identifican las posibles falencias y amenazas a las que está expuesta la organización, que puedan afectar el buen desempeño de la misma.

c) Actividades de Control.

Las actividades de control son las políticas y los procedimientos que ayudan a asegurar que se lleven a cabo las instrucciones de la dirección de la empresa. Ayudan a asegurar que se tomen las medidas necesarias para controlar los riesgos relacionados con la consecución de los objetivos de la empresa. Hay actividades de control en toda la organización, a todos los niveles y en todas las funciones. [8]

TIPOS DE ACTIVIDADES DE CONTROL

Existen muchas descripciones de tipos de actividades de control, que incluyen desde controles preventivos a controles detectivos y correctivos, controles manuales, controles informáticos y controles de dirección.

Algunos ejemplos:

Análisis efectuados por la dirección.- Los resultados obtenidos se analizan comparándolos con los presupuestos, las previsiones, los resultados de

ejercicios anteriores y de los competidores, con el fin de evaluar en que medida se están alcanzando los objetivos.

Gestión directa de funciones por actividades.- Los responsables de las diversas funciones o actividades revisan los informes sobre resultados alcanzados.

Proceso de información.- Se aplican una serie de controles para comprobar la exactitud, totalidad y autorización de las transacciones. Se controla el desarrollo de nuevos sistemas y la modificación de los existentes, al igual que el acceso a los datos, archivos y programas informáticos.

Controles físicos.- Los equipos de fabricación, las inversiones financieras, la tesorería y otros activos son objeto de protección y periódicamente se someten a recuentos físicos cuyos resultados se comparan con las cifras que figuran en los registros de control.

Indicadores de rendimiento.- El análisis combinado de diferentes conjuntos de datos (operativos o financieros) junto con la puesta en marcha de acciones correctivas, constituyen actividades de control.

Segregación de funciones.- Con el fin de reducir el riesgo de que se cometan errores o irregularidades, las tareas se reparten entre los empleados.

INTEGRACIÓN DE LAS ACTIVIDADES DE CONTROL CON LA EVALUACIÓN DE RIESGOS.

De forma paralela a la evaluación de los riesgos, la dirección deberá establecer y aplicar el plan de acción necesario para afrontarlos. Una vez identificadas, estas acciones también serán útiles para definir las operaciones de control que se aplicarán para garantizar su ejecución de forma correcta y en el tiempo deseado.

COMO EVALUAR LAS ACTIVIDADES DE CONTROL

Las actividades de control tienen que evaluarse en el contexto de las directrices establecidas por la dirección para afrontar los riesgos relacionados con los objetivos de cada actividad importante. La evaluación, por lo tanto, tendrá en cuenta si las actividades de control están relacionadas con el proceso de evaluación de riesgo y si son apropiadas para asegurar que las directrices de la dirección se cumplan. Dicha evaluación se efectuará para cada actividad importante, incluidos los controles generales de los sistemas informáticos. La evaluación deberá tener en cuenta no solamente si las actividades de control empleadas son relevantes en base al proceso de evaluación de riesgos realizando, sino también si se aplican de manera correcta. [9]

Estas actividades de control son las que indican cual es el camino a seguir para el desarrollo de las actividades normales de las organizaciones y estas sujetas a cambios de acuerdo con las exigencias del entorno en que se desempeña o se mueve una compañía.

d) Información y Comunicación.

Se debe identificar, recopilar y comunicar información pertinente en forma y plazo que permitan cumplir a cada empleado con sus responsabilidades. Los sistemas informáticos producen informes que contienen información operativa, financiera y datos sobre el cumplimiento de las normas que permite dirigir y controlar el negocio de forma adecuada. [8]

Los empleados tienen que comprender cuál es su papel en el sistema de Control Interno y cómo las actividades individuales están relacionadas con el trabajo de los demás. Asimismo, tiene que haber una comunicación eficaz con terceros, como clientes, proveedores, organismos de control y accionistas.

CALIDAD DE LA INFORMACIÓN

La calidad de la información generada por los diferentes sistemas afecta la capacidad de la dirección de tomar decisiones adecuadas al gestionar y controlar las actividades de la entidad. Resulta imprescindible que los informes ofrezcan suficientes datos relevantes para posibilitar un control eficaz.

Contenido ¿Contiene toda la información necesaria?

Oportunidad ¿Se facilita en el tiempo adecuado?

Actualidad ¿Es la más reciente disponible?

Exactitud ¿Los datos son correctos?

Accesibilidad ¿Puede ser obtenida fácilmente por las personas adecuadas?

COMUNICACIÓN INTERNA

Además, de recibir la información necesaria para llevar a cabo sus actividades, todo el personal, especialmente los empleados con responsabilidades importantes deben tomar en serio sus funciones comprometidas al Control Interno.

Cada función concreta ha de especificarse con claridad, cada persona tiene que entender los aspectos relevantes del sistema de Control Interno, como funcionan los mismos, saber cuál es su papel y responsabilidad en el sistema.

Asimismo, el personal tiene que saber cómo sus actividades están relacionadas con el trabajo de los demás, esto es necesario para conocer los problemas y determinar sus causas y la medida correctiva adecuada, El personal debe saber los comportamientos esperados, aceptables y no aceptables.

Los empleados también necesitan disponer de un mecanismo para comunicar información relevante a los niveles superiores de la organización, los empleados de primera línea, que manejan aspectos claves de las actividades todos los días, generalmente son los mas capacitados para reconocer los problemas en el momento que se presentan. Deben haber líneas directas de comunicación para que esta información llegue a niveles superiores, y por otra parte debe haber disposición de los directivos para escuchar.

COMUNICACIÓN EXTERNA

Los clientes y proveedores podrán aportar información de gran valor sobre el diseño y la calidad de los productos o servicios de la empresa, permitiendo que la empresa responda a los cambios y preferencias de los clientes. Por otra parte toda persona deberá entender que no se tolerarán actos indebidos, tales como sobornos o pagos indebidos.

COMO EVALUAR LA INFORMACIÓN Y COMUNICACIÓN

Se deberá considerar la adecuación de los sistemas de información y la comunicación a las necesidades de la entidad, a continuación se relacionan algunos aspectos posibles a considerar:

Información.

- La obtención de información externa e interna y el suministro a la dirección de los informes necesarios sobre la actuación de la entidad en relación a los objetivos establecidos.
- El suministro de información a las personas adecuadas, con el suficiente detalle y oportunidad.
- El desarrollo o revisión de los sistemas de información, basado en un plan estratégico para los sistemas de información.
- El apoyo de la dirección al desarrollo de los sistemas de información necesarios.

Comunicación.

- La comunicación eficaz al personal, de sus funciones y responsabilidades de control.
- El establecimiento de líneas de comunicación para la denuncia de posibles actos indebidos.
- La sensibilidad de la dirección a las propuestas del personal respecto de formas de mejorar la productividad, la calidad, etc.
- La adecuación de la comunicación horizontal. [9]

La información debe ser veraz y oportuna para permitir que la toma de decisiones se realice en forma adecuada.

e) Supervisión o Monitoreo.

Los sistemas de control interno requieren supervisión, es decir, un proceso que comprueba que se mantiene el adecuado funcionamiento del sistema a lo largo del tiempo. Esto se consigue mediante actividades de supervisión continuada, evaluaciones periódicas o una combinación de ambas cosas. La supervisión continuada se da en el transcurso de las operaciones. Incluye tanto las actividades normales de dirección y supervisión, como otras actividades llevadas a cabo por el personal en la realización de sus funciones. El alcance y la frecuencia de las evaluaciones periódicas dependerán esencialmente de una evaluación de los riesgos y de la eficacia de los procesos de supervisión continuada. Las deficiencias detectadas en el control interno deberán ser notificadas a niveles superiores, mientras que la alta dirección y el consejo de administración deberán ser informados de los aspectos significativos observados. [8]

SUPERVISIÓN CONTINUA

Existe una gran variedad de actividades que permiten efectuar un seguimiento de la eficacia del Control Interno, como comparaciones, conciliaciones, actividades corrientes de gestión y supervisión así como otras actividades rutinarias.

ALCANCE Y FRECUENCIA

El alcance y la frecuencia de la evaluación del Control Interno variarán según la magnitud de los riesgos objeto de control y la importancia de los controles para la reducción de aquellos. Así los controles actuarán sobre los riesgos de mayor prioridad y los más críticos para la reducción de un determinado riesgo serán objeto de evaluación más frecuente.

- El nivel de apertura y eficacia de las líneas de comunicación con clientes, proveedores y terceros.
- El nivel de comunicación a terceros de las normas éticas de la entidad.
- La realización oportuna y adecuada del seguimiento por parte de la dirección de las informaciones obtenidas de terceros, clientes, organismos de control, etc. [9]

EL PROCESO DE EVALUACIÓN

La evaluación de un Sistema de Control constituye un proceso, si bien los enfoques y técnicas varían, debe mantenerse una disciplina en todo el proceso. El evaluador deberá entender cada una de las actividades de la

entidad y cada componente del Sistema de Control Interno objeto de la evaluación. Conviene centrarse en el funcionamiento teórico del sistema, es decir en su diseño, lo cual implicará conversaciones previas con los empleados de la entidad y la revisión de la documentación existente.

La tarea del evaluador es averiguar el funcionamiento real del sistema. Es posible que, con el tiempo determinados procedimientos diseñados para funcionar de un modo determinado se modifiquen para funcionar de otro modo, o simplemente se dejen de realizar. A veces se establecen nuevos controles, no conocidos por las personas que en un principio, describieron el sistema, por lo que no se hallan en la documentación existente, a fin de determinar el funcionamiento real del sistema, se mantendrán conversaciones con los empleados que aplican y se ven afectados por los controles, se revisarán los datos registrados sobre el cumplimiento de los controles, o una combinación de estos dos procedimientos.

El evaluador analizará el diseño del Sistema de Control Interno y los resultados de las pruebas realizadas. El análisis se efectuará bajo la óptica de los criterios establecidos, con el objeto último de determinar si el sistema ofrece una seguridad razonable respecto a los objetivos establecidos.

4.2.3. Planeación Estratégica

4.2.3.1. Misión

Es la razón de ser de la empresa considerando sobre todo la atractividad del negocio.

En la misión de la empresa investigada de la industria se hace un análisis del macro y micro entorno que permita construir el escenario actual y

posible, para que sea posible ver con mayor énfasis la condición y razón de ser de la empresa en dicho mercado. [2]

4.2.3.2. Visión

Descripción de un escenario altamente deseado por la dirección general de una organización. Capacidad de ver más allá del tiempo y el espacio, para construir en la mente un estado futuro deseable que permita tener una claridad sobre lo que se quiere hacer y a dónde se quiere llegar en una organización. [10]

4.2.3.3. Valores

Los valores, como herramientas o enfoques gerenciales, han venido ocupando un lugar cada vez más relevante en las teorías y prácticas de la administración en los últimos años. Athos y Pascale definen los valores corporativos como “reglas o pautas mediante las cuales una compañía exhorta a sus miembros a tener comportamientos consistentes con su sentido de existencia (orden, seguridad y desarrollo). Son propósitos supremos a los cuales la organización y sus miembros deben dedicar toda su energía”. [11]

4.2.3.4. Cadena de Valor

La cadena de valor ayuda a determinar las actividades que permiten generar una Ventaja Competitiva sustentable (también expresado por M. Porter). Tener una ventaja competitiva es tener una rentabilidad relativa

superior a los rivales en el sector industrial en el cual se compete. Rentabilidad significa un margen entre los ingresos y los costos. Cada actividad que realiza la empresa debe generar el mayor posible. De no ser así, debe costar lo menos posible, con el fin de obtener un margen superior al de los rivales. Las Actividades de la cadena de valor son múltiples y además complementarias (relacionadas). El conjunto de actividades de valor que decide realizar una unidad de negocio es a lo que se le llama estrategia competitiva (también expresado por M. Porter) o estrategia del negocio (diferente a las estrategias corporativas o a las estrategias de un área funcional). [12]

5. MODELO PROPUESTO

A continuación se presentan las etapas del modelo, con una breve descripción de lo que se haría en cada una y sus entradas, así como lo que se espera obtener de cada una de ellas.

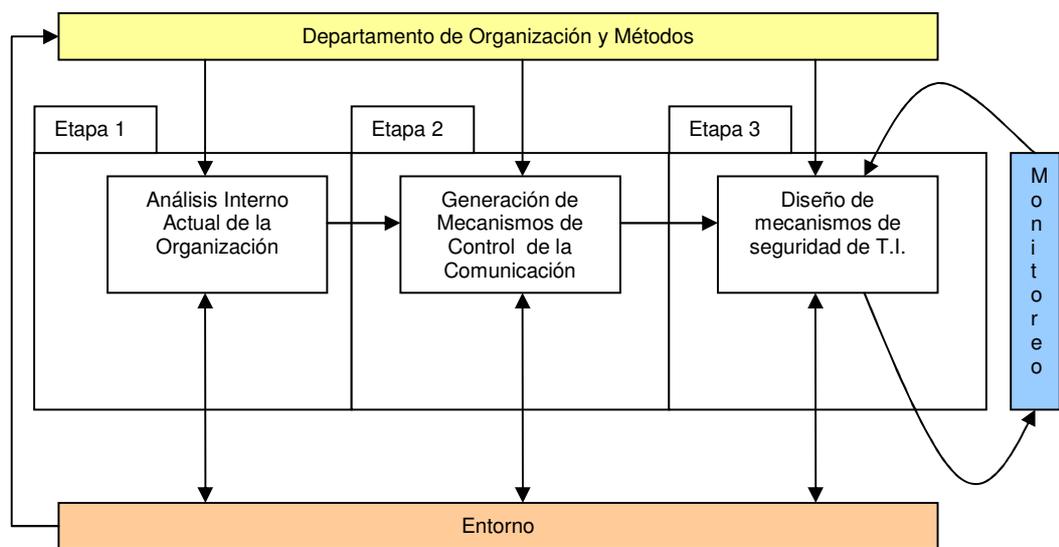


Gráfico 2. Modelo de Gestión Propuesto

El modelo propuesto consta de tres etapas las cuales son:

- Análisis interno actual de la organización
- Generación de mecanismos de control de la comunicación
- Diseño de mecanismos de seguridad de T.I.

A lo largo de todo el modelo se ven aplicados los conceptos del MSV [1] y COSO con sus cinco componentes del control interno [4]. Se aplica también el análisis externo a lo largo de todo el modelo con el fin de visualizar lo que está sucediendo en el ambiente y las mejoras prácticas poderlas aplicar para el beneficio de la compañía.

En la primera etapa se realiza un análisis de la situación actual de la compañía, de donde se obtendrá la información prioritaria con la que se trabajará en el desarrollo de este trabajo. Esa información incluye: Misión, Visión, Valores, Cadena de Valor [2], Procesos del núcleo y la Situación Actual del entorno informático.

En la segunda etapa se generarán los mecanismos de control de la comunicación teniendo en cuenta toda la información recolectada en la primera, con el fin de garantizar una comunicación oportuna y segura entre los niveles de la compañía que la requieran.

En la tercera etapa se diseñarán los mecanismos de seguridad que conlleven a la efectiva y eficiente comunicación entre las sedes, en esta etapa se propone adquirir todos los dispositivos de hardware y software que permitan el cumplimiento del objetivo planteado en este trabajo.

5.1. Análisis Interno Actual de la Organización

5.1.1. Entradas

Para alcanzar este objetivo se tienen las siguientes entradas:

- Hardware y software actual de la compañía
- Antecedentes de la compañía
- Planeación estratégica
- Cadena de Valor

5.1.2. Metodología

A través del departamento de Organización y Métodos se canalizan las características del entorno de las compañías del sector y aquí se analizarán los aspectos relacionados con los objetivos del negocio.

Se analizan: Misión, Visión, Valores, Cadena de Valor [2], Procesos del núcleo y la Situación Actual del entorno informático. De toda la información obtenida se construye una matriz de riesgos y se identifican las necesidades del área de T.I.

5.1.3. Salidas

- Necesidades del área de T.I.
- Identificación de riesgos

5.2. **Generación de Mecanismos de Control de la Comunicación**

5.2.1. Entradas

- Necesidades del área de T.I.
- Identificación de riesgos

5.2.2. Metodología

Al igual que en la primera etapa el departamento de organización y métodos interioriza hacia la compañía todos los factores correspondientes para que el modelo de comunicación sea viable y sostenible, basados en la infraestructura tecnológica que posee la organización. De aquí surgirán las políticas de seguridad

y control informático teniendo en cuenta los componentes del control interno mencionados en el marco teórico de este trabajo.

5.2.3. Salidas

- Estrategias para mitigar los riesgos
- Reestructuración de la infraestructura tecnológica
- Políticas de control en las comunicaciones

5.3. Diseño de Mecanismo de Seguridad de T.I.

5.3.1. Entradas

- Estrategias para mitigar los riesgos
- Reestructuración de la infraestructura tecnológica
- Políticas de control en las comunicaciones y seguridad informática
- Análisis de las políticas actuales existentes

5.3.2. Metodología

Una vez obtenidas las políticas de seguridad y control de la información y analizada la infraestructura tecnológica se procede a interiorizarla en la organización, procediendo con la adquisición de los recursos informáticos para la puesta en marcha de las mismas.

5.3.3. Salidas

- Revisión de las políticas de sistemas
- Revisión de Políticas de control y seguridad informática
- Adquisición de tecnología para proveer seguridad informática

6. IMPLEMENTACIÓN DEL MODELO PROPUESTO EN UNA SITUACIÓN REAL

El modelo diseñado fue aplicado hasta la segunda etapa en la empresa Autobol S.A.

6.1. Etapa 1 - Análisis Interno Actual de la Organización

6.1.1. Entradas

Autobol S.A., se dedica a la venta de vehículos marca Mazda y también ofrece servicios de mantenimiento, venta de repuestos y combustibles. Actualmente su única oficina funciona en la ciudad de Cartagena de Indias y la idea principal de sus accionistas es la de expandir su mercado y abrir una nueva oficina que ofrezca los mismos servicios en la ciudad de Valledupar, para lo cual se hace necesario implementar una completa infraestructura de negocio que le permita a Autobol S.A. surgir en un mercado en el cual la marca Mazda no había incursionado.

6.1.1.1. Antecedentes

Presentación de la Organización

La construcción de Autobol S.A. - Automotora de Bolívar -, ha significado una tarea continua de esfuerzos para la culminación de un sueño compartido.

En 1969 el Sr. Cristóbal López Vargas junto con tres socios, deciden responder a los habitantes de la ciudad, frente a la necesidad de adquirir sus vehículos sin

tener que desplazarse al resto del país, y así mismo ofrecer un servicio integral que incluyera mantenimiento, venta de repuestos y combustible, con el objetivo de mejorar el bienestar y la calidad de vida de las comunidades de su entorno, así como de lograr respuestas para las urgencias esenciales en cuanto al medio de transporte.

Es así, como se consolida la constitución de la empresa que lleva por nombre Autobol Ltda., la cual comienza a operar con un total de 10 empleados, comprometidos con su desarrollo y con el ideal de hacerla líder en el mercado, a través de buen servicio y atención.

En 1990 la empresa obtuvo un avanzado desarrollo en sus ventas, con un promedio de veinte (20) vehículos vendidos por mes, marca Mazda, generando grandes utilidades y abriendo nuevos horizontes de ventas. La empresa introdujo en este año una nueva marca de vehículos -Nissan- permitiendo así el crecimiento de las ventas y por ende el sostenimiento como únicos distribuidores autorizados de estas dos marcas en la ciudad. Para este entonces, la empresa ya contaba con un total de 30 trabajadores, respondiendo efectivamente a la demanda.

En 1999 Autobol Ltda., pasa a ser constituida como una sociedad anónima mediante inscripción en la Cámara de Comercio de la ciudad, el 16 de abril del mismo año. La empresa mantiene entonces su filosofía encaminada hacia los clientes y todos sus trabajadores - los cuales a la fecha ascienden entonces a cuarenta (40) - giran entorno a estos con el fin de satisfacer oportunamente su necesidad de transporte y reparación de vehículos.

En el 2005 la empresa decide solo mantener la distribución y mantenimiento exclusivo de la marca Mazda en la ciudad de Cartagena, dejando atrás la marca Nissan. Esto con el objetivo de especializarse y atender mejor su nicho de

mercado. El objetivo es trabajar arduamente por obtener la certificación de calidad en sus procesos de “Entrega Perfecta” “SUG” y “5´s”, procesos que son calificados y otorgados directamente por la casa matriz CCA (Compañía Colombiana Automotriz).

En el 2006 Autobol S.A., trabaja arduamente por mantenerse como líder en el mercado, buscando mejorar y mantener la excelencia operacional y de servicios que incidirán directamente hacia la plena satisfacción de todos sus clientes locales.

El gerente de la compañía desde su proyecto e inauguración ha sido el Sr. Cristóbal López Vargas, quien ha entregado gran parte de su vida al negocio, siendo reconocido localmente como una de las personas más perseverantes e instruidas en temas automovilísticos.

6.1.1.2. Misión de Autobol S.A.

“Orientar y satisfacer las necesidades de nuestros clientes, ofreciéndoles asesoría personalizada en la venta de vehículos, además de una amplia gama de servicios constituidos por el mantenimiento, venta de repuestos y suministro de combustible, brindándoles productos de óptima marca y calidad, comprometiendo nuestros recursos humanos para el logro de una mayor satisfacción”.

6.1.1.3. Visión de Autobol S.A.

“Ser la empresa más eficiente, dinámica y rentable entre los grandes concesionarios nacionales, manejando en forma estratégica nuestros diferentes servicios de tal manera que garanticemos la total satisfacción de nuestros clientes, el desarrollo sostenido de nuestros empleados, mayor valor para nuestros accionistas y así contribuir más en el bienestar de nuestra sociedad en general”.

6.1.1.4. Valores de Autobol S.A.

- Responsabilidad
- Trabajo en Equipo
- Honestidad
- Respaldo
- Respeto y
- Eficiencia

6.1.1.5. Cadena de Valor Autobol S.A.

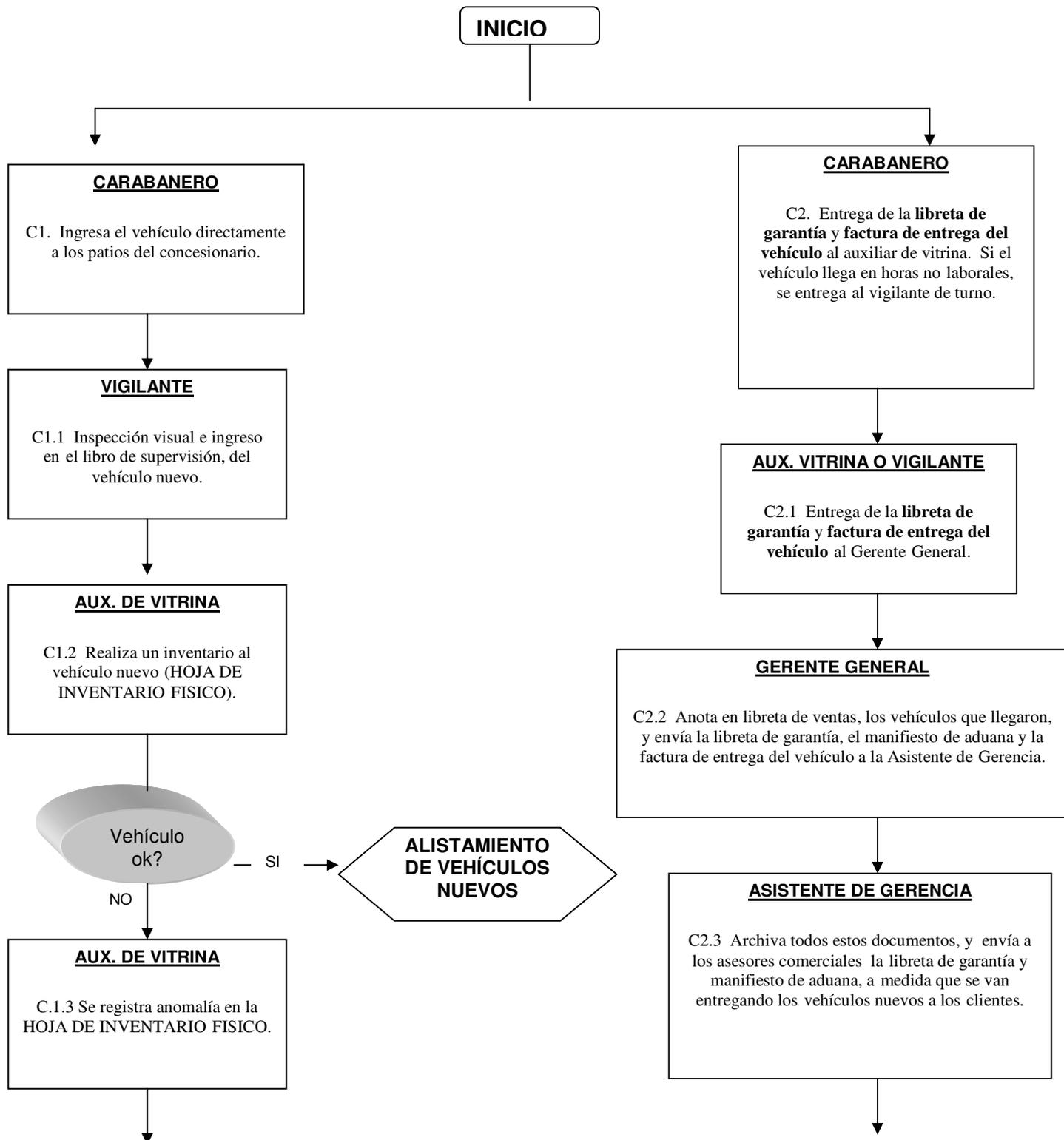


Gráfico 3. Cadena de Valor de Autobol S.A.

6.1.1.6. Proceso de Recepción de Vehículos Nuevos

Los vehículos llegan a nuestra empresa ensamblados, desde el proveedor que es la Compañía Colombiana Automotriz (CCA), a través de la empresa transportadora Carabanero. En el momento en que el vehículo ingresa a la compañía se le da entrada en el inventario, donde se registran todos los datos del mismo. Esto lo hace la secretaria de ventas, la cual adicionalmente, ingresa los datos del cliente, vía Web, en el modulo de vehículos de la aplicación Sistema SINCO, ubicada en el portal de la CCA, para efectos de la garantía del vehículo.

El área de sistemas interviene en este proceso dando apoyo a través de las aplicaciones de Inventario y garantizando el acceso a SINCO.



AUX. DE VITRINA
C1.4 Envía al Taller una copia de la HOJA DE INVENTARIO FISICO, para la corrección del daño del vehículo. La original , la archiva.

ALISTAMIENTO DE VEHÍCULOS NUEVOS

FIN

ASESOR COMERCIAL
C2.4 Al momento de la entrega del vehículo, el cliente debe firmar el cupón de la libreta de garantía.

ASESOR COMERCIAL
C2.5 Entrega a la secretaria de gerencia general, el cupón de la garantía firmado por el cliente.

SECRETARIA DE GERENCIA GENERAL
C2.6 Registro de propietarios en SINCO.

SECRETARIA DE GERENCIA GENERAL
C2.7 Entrega cupones de garantías a la asistente de gerencia.

ASISTENTE DE GERENCIA
C2.8 Archiva el cupón de la garantía en el fólder del cliente.

ASISTENTE DE GERENCIA
C2.9 Saca copia de la factura de entrega de vehículo, y la envía a Contabilidad.

ASISTENTE DE GERENCIA
C2.10 Envía la factura de entrega de vehículo original a la secretaria de gerencia general, la cual procede a archivarla.

Gráfico 4. Proceso de Recepción de Vehículos Nuevos

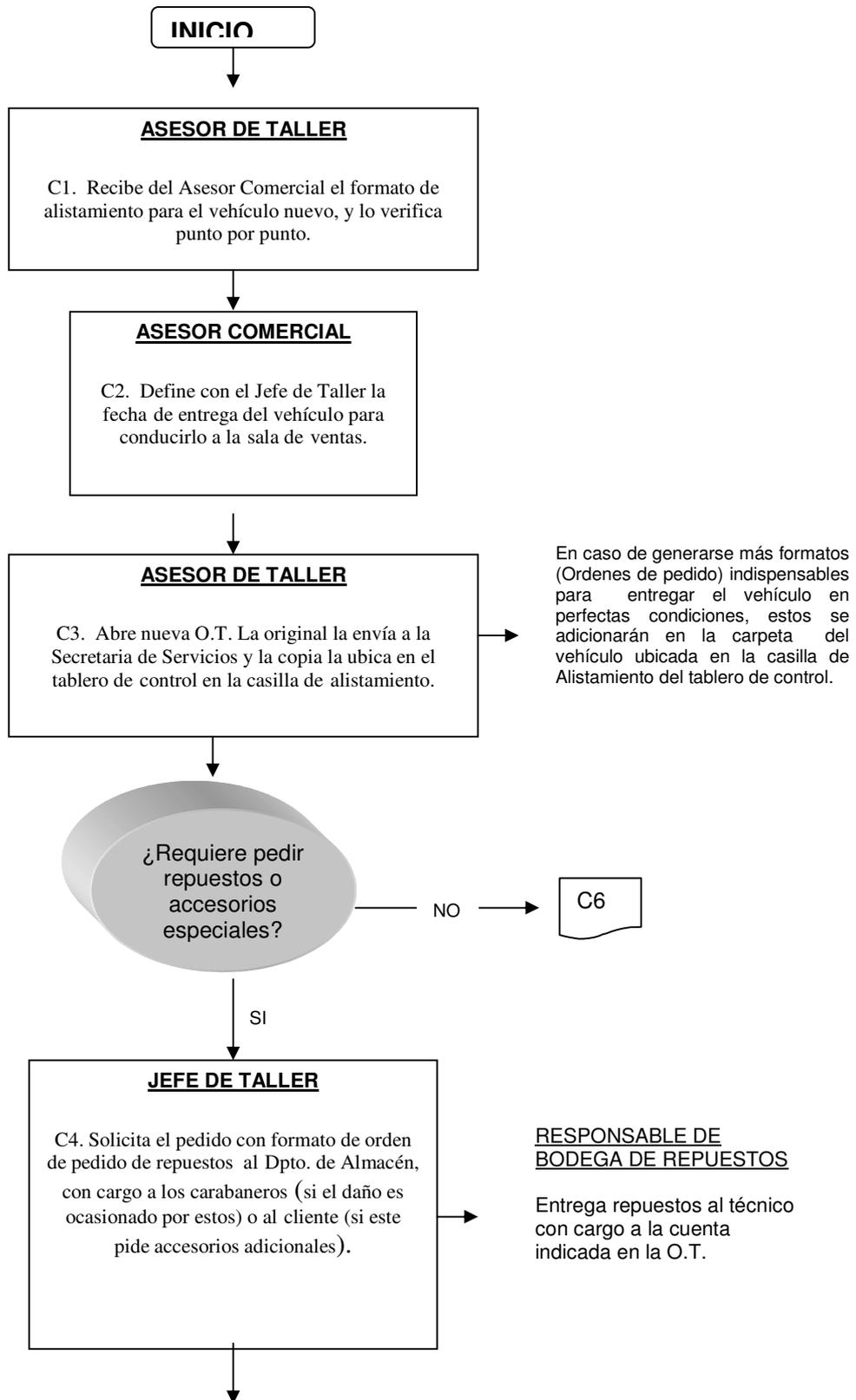
6.1.1.7. Proceso De Alistamiento De Vehículos Nuevos

Ingresado el vehículo al sistema por la aplicación de Inventario, se procede a realizar el alistamiento o acondicionamiento de este para su venta, abriéndole una orden de trabajo OT, la cual lleva un código de facturación acompañada del número de motor del vehículo.

Si el Cliente hace una solicitud de repuestos o de un accesorio adicional, este se diligencia a través de un formato de orden de pedido de repuestos al departamento de almacén, estos facturan internamente y cargan el valor del pedido a la orden de trabajo del vehículo.

Cuando el vehículo llega con alguna anomalía por parte de la empresa transportadora –Carabaneros-, se realiza su arreglo y el valor se le carga a la empresa de transporte. Finalmente la facturación se realiza desde el modulo de contabilidad.

La aplicación que maneja el proceso de inventario y facturación de Autobol, es apoyada por el Área de Sistemas, quien asegura su correcto funcionamiento e integridad de los datos que proporcionan.



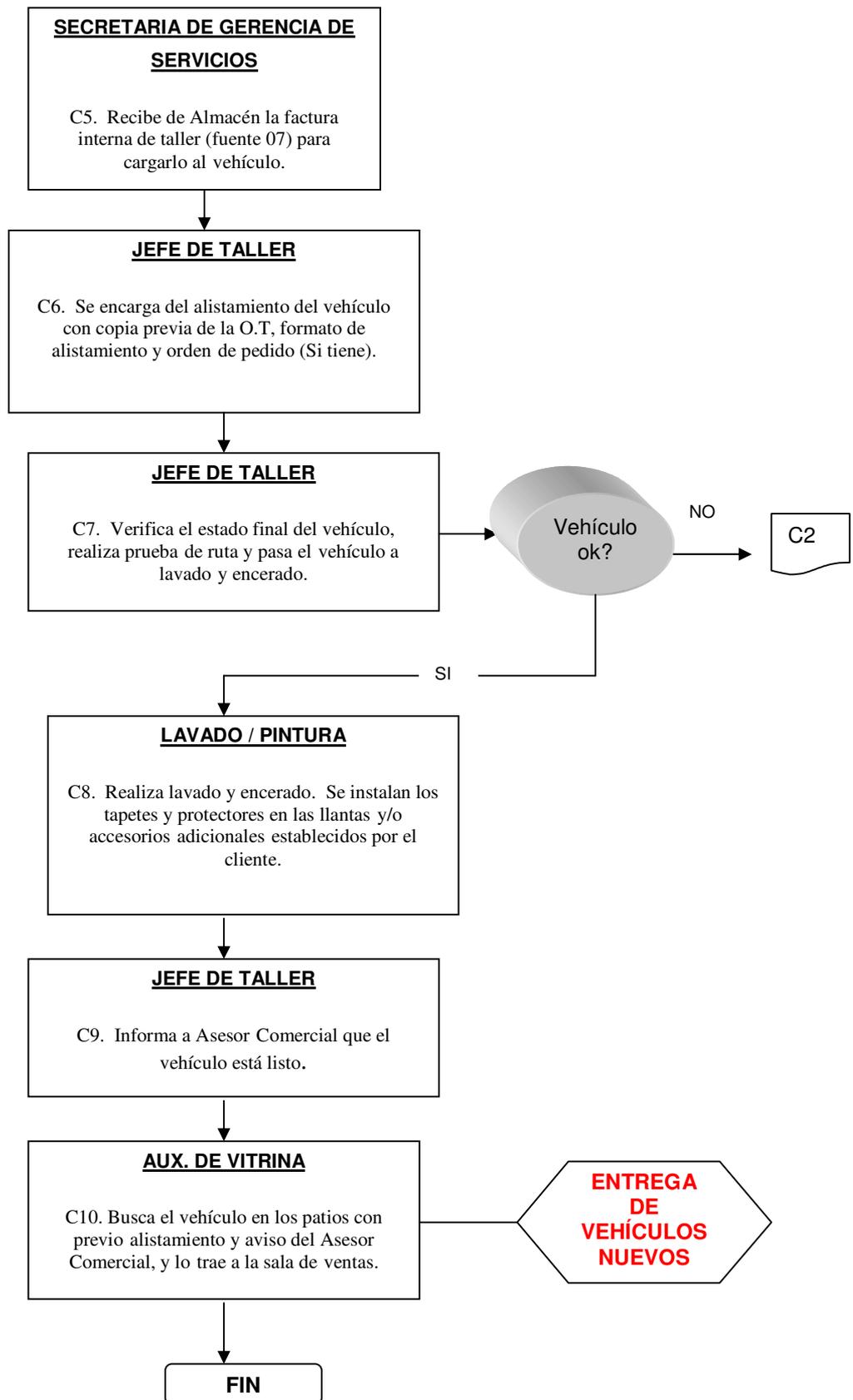


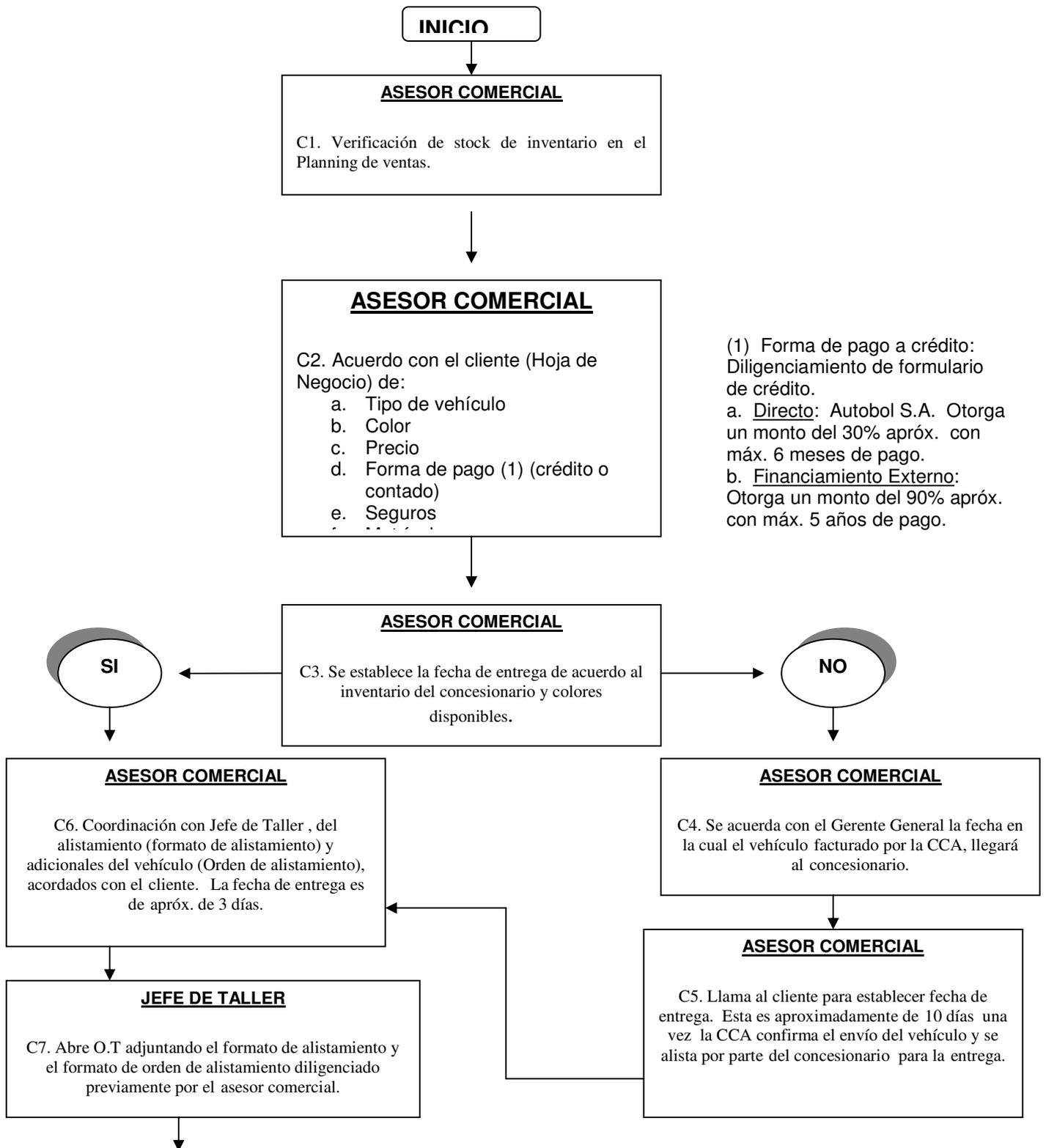
Gráfico 5. Proceso de Alistamiento de Vehículos Nuevos

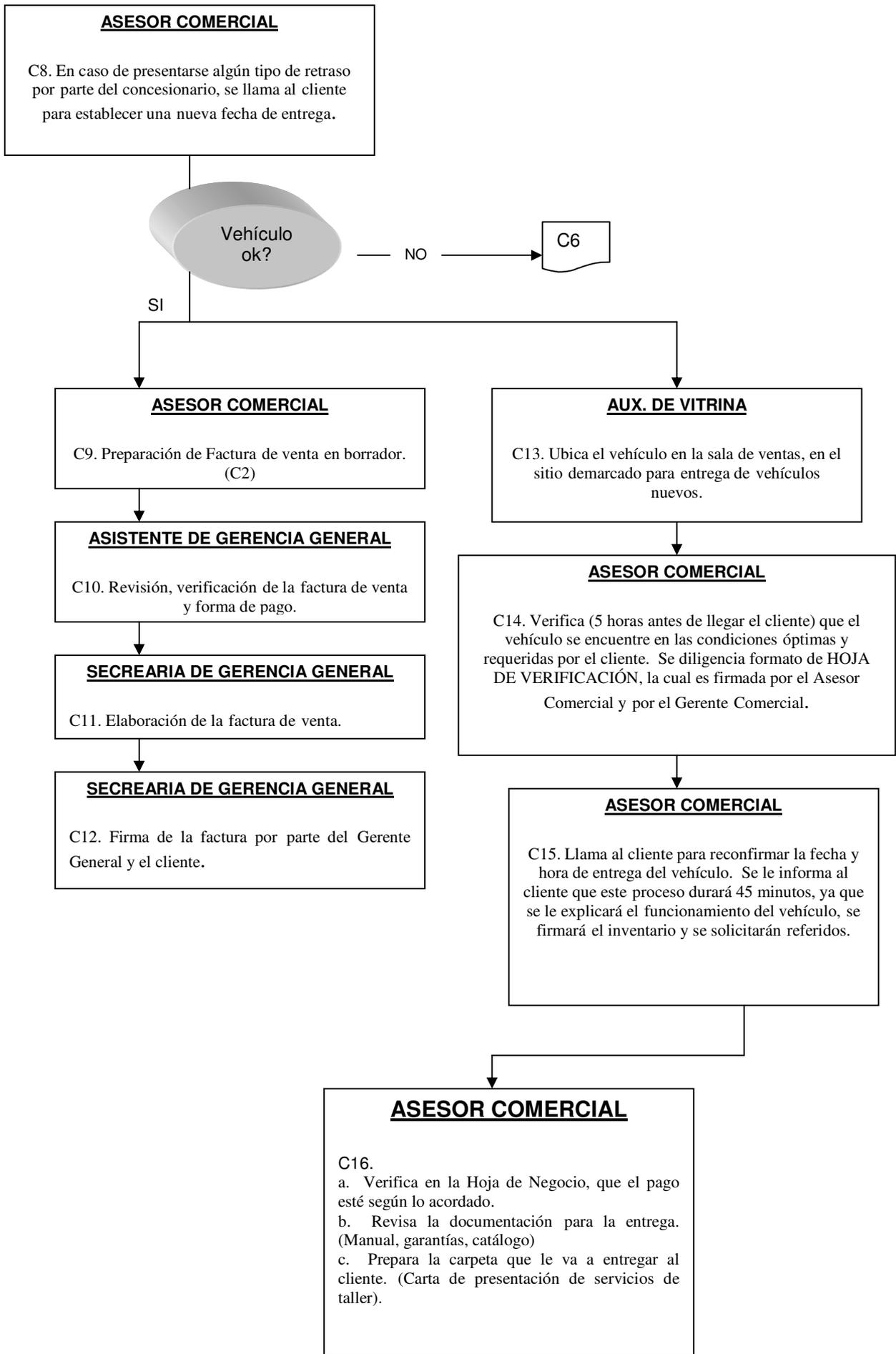
6.1.1.8. Proceso De Entrega De Vehículos Nuevo

Realizado el alistamiento, el vehículo esta presto para su facturación, en donde se le carga el valor de todo lo efectuado en el acondicionamiento, y queda listo para ser entregado al cliente.

La factura final del vehículo se realiza en la aplicación de Contabilidad obteniendo los datos del alistamiento de la aplicación de Inventario.

El área de sistema brinda soporte en todo este proceso desde la recepción del vehículo hasta la entrega del mismo, garantizando el buen funcionamiento de las aplicaciones de contabilidad e inventario.





ASESOR COMERCIAL

C8. En caso de presentarse algún tipo de retraso por parte del concesionario, se llama al cliente para establecer una nueva fecha de entrega.

Vehículo ok?

NO

C6

SI

ASESOR COMERCIAL

C9. Preparación de Factura de venta en borrador. (C2)

ASISTENTE DE GERENCIA GENERAL

C10. Revisión, verificación de la factura de venta y forma de pago.

SECRETARIA DE GERENCIA GENERAL

C11. Elaboración de la factura de venta.

SECRETARIA DE GERENCIA GENERAL

C12. Firma de la factura por parte del Gerente General y el cliente.

AUX. DE VITRINA

C13. Ubica el vehículo en la sala de ventas, en el sitio demarcado para entrega de vehículos nuevos.

ASESOR COMERCIAL

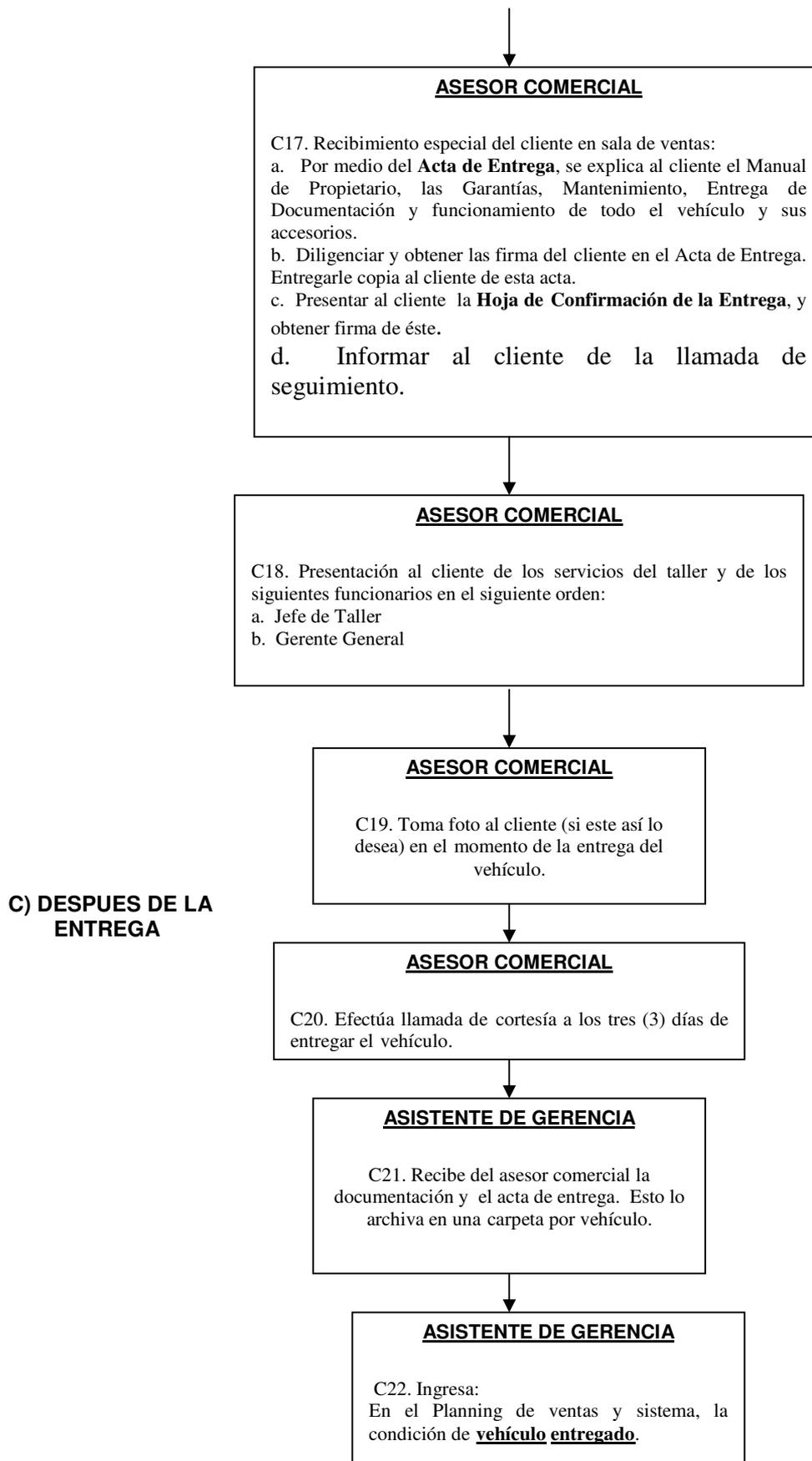
C14. Verifica (5 horas antes de llegar el cliente) que el vehículo se encuentre en las condiciones óptimas y requeridas por el cliente. Se diligencia formato de HOJA DE VERIFICACIÓN, la cual es firmada por el Asesor Comercial y por el Gerente Comercial.

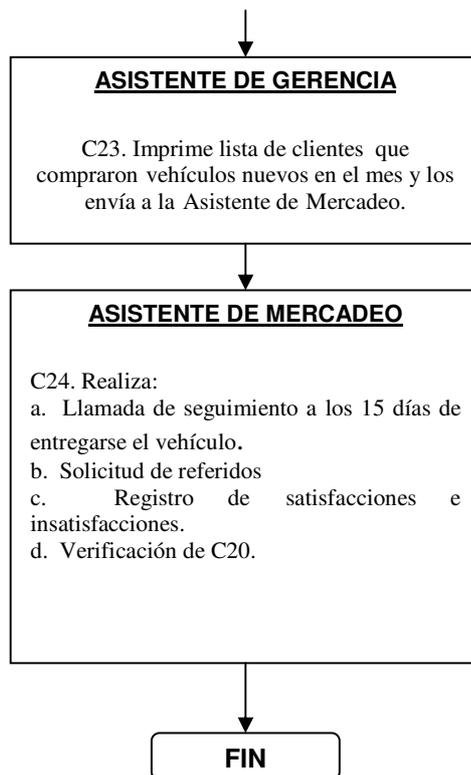
ASESOR COMERCIAL

C15. Llama al cliente para reconfirmar la fecha y hora de entrega del vehículo. Se le informa al cliente que este proceso durará 45 minutos, ya que se le explicará el funcionamiento del vehículo, se firmará el inventario y se solicitarán referidos.

ASESOR COMERCIAL

C16.
 a. Verifica en la Hoja de Negocio, que el pago esté según lo acordado.
 b. Revisa la documentación para la entrega. (Manual, garantías, catálogo)
 c. Prepara la carpeta que le va a entregar al cliente. (Carta de presentación de servicios de taller).





Gráfica 6. Proceso de Entrega de Vehículos Nuevos

6.1.1.9. Proceso De Venta De Repuestos Para Vehículos Mazda

AUTOBOL además de comercializar los vehículos Mazda nuevos, también ofrece los repuestos automotriz originales de los mismo, brindando productos de calidad y garantizados, que se reflejan en la satisfacción del cliente.

Los repuestos, los provee la Compañía Colombiana Automotriz (CCA), los cuales son despachados por medio de pedidos que realiza el personal del almacén de repuestos de Autobol S.A..

Los clientes pueden ser internos o externos, internos el taller de servicios de la empresa, que ofrece el servicio de mantenimiento y reparación de vehículos Mazda, y externos los clientes que se acercan al almacén de repuestos de Autobol S.A. para adquirir los repuestos para sus vehículos.

6.1.1.10. Proceso En La Estación De Servicios

AUTOBOL cuenta con una Estación de Servicios, donde se comercializa la venta de combustible, y todos los productos que requiere un vehículo para su óptimo funcionamiento motriz.

El proveedor que suministra el combustible y demás productos, es CHEVRON PETROLEUM TEXACO.

El Administrador de la Estación hace una orden de pedido dirigida a CHEVRON PETROLEUM TEXACO, quien despacha el producto solicitado.

Los clientes a los que se les presta el servicio, pueden ser interno o externos. Internos, para uso en el taller de servicios o para el alistamiento de los vehículos nuevos, externos los cliente que hacen uso de la estación de servicios ubicada a las afueras de la empresa.

6.1.1.11. Situación Actual Del Entorno Informático

6.1.1.11.1. Red de comunicación de datos

- Red lógica

La red de comunicación de datos de Autobol S.A. se encuentra soportada por una red de cableado estructurado con cables UTP de categoría 5e, los cuales cubren 13 puntos lógicos.

Ver [Red Autobol Actual.jpg](#)

- Red LAN

La topología de la red es de tipo estrella, la cual es soportada por los siguientes equipos:

- Un switch 3COM 10/100 Mbps ethernet (24 puertos)
- Un switch Netgear 10/100 Mbps Ethernet (16 puertos)
- Un hub 3COM 10/100 Mbps Ethernet (8 puertos)

- Protocolo

Se utiliza el protocolo TCP/IP versión 4 con direcciones de red tipo C dentro del rango 192.168.0.1 y 192.168.0.255 con máscara de subred 255.255.255.0

- Conexión a Internet

Características:

- Velocidad: 256 kbps
- Reuso: 1:1
- ISP: Telecom
- URLs: Websense
- Tipo: Dedicado
- Protocolo: TCP/IP
- Enrutador : Cisco (Propiedad del ISP)
- Canal: Fibra óptica
- La administración del servicio está en manos de Telecom
- Se tienen disponibles 25 MB para la página web.

- Correo electrónico

Actualmente se está implementando el dominio para Autobol S.A., esta actividad se está realizando con la empresa Telecom. Se asignará una dirección de dominio para la página web y correo electrónico.

No existen cuentas de correo creadas para los usuarios, por lo tanto no se ha dado capacitación en este tema.

No existen políticas para el uso y creación de cuentas de correo electrónico, se tiene planeada la creación de 15 cuentas de correo electrónico.

- Se piensa usar el dominio www.autobol.com
- POP3 y SMTP: correo.telecom.com.co

6.1.1.11.2. Hardware

Está compuesto por los siguientes elementos:

- 1 Servidor con windows 2003 server
- 15 equipos de computo en red
- 5 equipos de computos independientes
- 3 equipos portátiles
- 1 equipo de computo analizador de gases
- 1 equipo de computo para alineación
- 1 equipo de computo diagnosticador de fallas
- 12 ups de 650
- 1 reversion ups
- 7 impresoras matriz de punto epson lx-300
- 3 impresoras hp deskjet 3940
- 1 impresora hp deskjet 810c
- 1 impresora hp deskjet 845
- 1 impresora epson stylus sc42
- 1 impresora epson fx – 2190 carro ancho

6.1.1.11.3. Políticas de sistemas

El departamento de sistemas no tiene en la actualidad políticas de sistemas.

6.1.1.11.4. Políticas de seguridad

El departamento de sistemas no tiene en la actualidad políticas de sistemas.

6.1.2. Metodología

Mediante la utilización del ambiente de control [8] se analizó el entorno de la organización y se procedió a incluir los elementos de la organización referentes a la misión, la misión, sus valores, la cadena de valor y la situación actual del ambiente informático.

A continuación se presenta el análisis y comparación adelantados a través de una matriz de riesgos, como lo plantea la evaluación de riesgos[9], en la cual se identifican y se muestra la causa que los genera, su impacto y a quienes afecta.

6.1.3. Salidas

6.1.3.1. Matriz de Riesgos

En la cual se identifican los riesgos de acuerdo a la metodología propuesta

RIESGO	IMPACTO	CAUSAS QUE LO GENERAN	A QUIEN AFECTA	PROBABILIDAD
Divulgación de información confidencial a otras empresas del sector	1	No existen restricciones en el uso y divulgación de la información propiedad de Autobol	A la organización, ya que la competencia podría tener acceso a la información de vital importancia	Media
Perdida de información	1	No existen medidas de contingencia para evitar perdida de información.	El área de sistemas y a todas las demás áreas que se vean involucradas	Media
Uso inadecuado de la información	2	No existen restricciones ni normas para el uso adecuado de la información	A todos los procesos de la organización	Media
Acceso no autorizado a la información	2	Falta de control y autenticación de las contraseñas de acceso	área de sistemas y a la organización	Alta
Retraso en la entrega de la información de una sede a otra	2	No existe una red de comunicación que interconecte a las dos sedes.	A los clientes y la Organización por incumplimiento con las tareas	Alta
Entrega de información desactualizada	1	No existe una red de comunicación que interconecte a las dos sedes y permita intercambiar información en tiempo real.	A los clientes y a todo funcionario en el desempeño de sus funciones	Media
Caída o Bajo rendimiento de la Red de Comunicación	2	Equipos con poca capacidad para obtener una conexión optima	Todas las áreas	Media
Incumplimiento a los clientes, o retardo en entrega de producto	1	No existe un canal de comunicación directo entre ambas sedes.	Cliente y Organización	Alta
No habilitación de punto de red de funcionario nuevo	3	No existencia de equipos de red, que permitan agregar otros puntos de red	Empleado y su área	Alta

Tabla 1. Matriz de Riesgos

6.1.3.2. Necesidades del área de T.I.

Las necesidades encontradas fueron:

- Necesidad de expansión en la red lógica de la sede de Cartagena.
- Necesidad de adquisición de hardware (servidor)
- Necesidad de crear la nueva infraestructura tecnológica para la sede de Valledupar.
- Necesidad de creación de la conexión entre las dos sedes.
- Necesidad de establecer controles para establecer la seguridad informática de la compañía.
- Necesidad de crear las políticas de sistemas

6.2. Etapa 2 – Generación de Mecanismos de Control de la Comunicación

6.2.1. Entradas

Las entradas para esta etapa son:

- La Matriz de Riesgos
- Necesidad de expansión en la red lógica de la sede de Cartagena.
- Necesidad de adquisición de hardware (servidor)
- Necesidad de crear la nueva infraestructura tecnológica para la sede de Valledupar.
- Necesidad de creación de la conexión entre las dos sedes.
- Necesidad de establecer controles para establecer la seguridad informática de la compañía.
- Necesidad de crear las políticas de sistemas

Las cuales fueron las salidas resultantes de la etapa Análisis Interno Actual de la organización.

6.2.2. Metodología

Teniendo en cuenta las entradas se procedió a analizarlas y a compararlas con los escenarios que están en el entorno de la organización y se propusieron las políticas de sistemas y las políticas de seguridad y control informático, en las cuales se pueden ver aplicadas funciones de control y monitoreo [8] con el fin de mantener la continuidad de los procesos y la permanencia del negocio en el tiempo.

6.2.3. Salidas

Las salidas para esta etapa son: las estrategias para mitigar los riesgos representadas en las políticas de control de acceso, la reestructuración de la infraestructura tecnológica representada en la situación propuesta del entorno informático y las políticas de control de las comunicaciones representadas en las políticas de sistemas y de seguridad y control informático.

6.2.3.1. Políticas de Control de Acceso

Control de acceso

Los controles de acceso lógico se utilizan con el fin de restringir o habilitar de alguna forma el tipo de acceso que los usuarios tienen a la información de propiedad de la compañía. Para conseguir esto el administrador de red debe garantizar que los perfiles asignados a los usuarios solo dispongan de la

información necesaria y la forma en que pueden utilizarla para el desarrollo de las labores de acuerdo a las funciones de los cargos.

Reducción del número de identificadores de usuarios privilegiados

El número de identificadores de usuarios privilegiados en el sistema debe ser mínimo, esto con el fin de mantener la confiabilidad del sistema. Con este fin solo se permitirán 3 cuentas de usuarios privilegiados trabajando en un mismo instante.

Restricción de tiempo para acceso de usuarios privilegiados

Al permitir que un usuario acceda al sistema como usuario privilegiado, se le debe indicar a este que lo está haciendo y que el tiempo permitido para su trabajo será de una hora.

Privilegios de acceso de usuario

El acceso normal de los usuarios debe estar restringido de acuerdo a la información en la que pueda trabajar dependiendo de las funciones de su cargo, así mismo se aplicará a las aplicaciones y comandos que podrá ejecutar.

Terminación de sesiones

Se consideran sesiones de usuarios inactivas a aquellas que no han tenido intercambio de información hacia o desde el usuario por cierto periodo de tiempo, teniendo en cuenta lo anterior el sistema terminará la sesión de un usuario cuando este detecte que se ha encontrado inactiva por más de 15 minutos.

Inhabilitación de identificadores de usuario

Todos los empleados que dejen laborar con Autobol S.A. deberán tener deshabilitados todos los identificadores de todos los sistemas de la compañía. Esta labor se deberá hacer inmediato a la notificación del jefe administrativo o antes de que el empleado salga de la compañía si así se notifica.

Eliminación de identificadores de usuario

El administrador del sistema deberá eliminar todos los identificadores de usuario y/o modificar los accesos a las aplicaciones y los permisos a los datos de los usuarios que cambian de responsabilidades en el trabajo. La notificación de cambio la debe hacer el jefe administrativo y este cambio se deberá hacer a más tardar al día siguiente de la notificación.

Software de control de acceso

El software de control de acceso se deberá utilizar en todo momento para permitir el ingreso a los equipos del centro de computo y a los equipos de escritorio que acceden a la red de la compañía.

Notificación de advertencia

Esta deberá ser la leyenda en las pantallas de inicio de las sesiones a los sistemas de Autobol S.A.

Este sistema está autorizado única y exclusivamente para ser utilizado por personal autorizado por Autobol S.A. y para propósitos de la compañía. El acceso realizado o intento de acceso, uso o modificación del sistema no autorizado, está terminalmente prohibido por Autobol S.A. El uso de este sistema puede ser monitoreado o registrado por razones administrativas o de seguridad.

6.2.3.2. Situación Propuesta Del Entorno Informático

Red de comunicación de Datos

Sede en Cartagena

- Red lógica

Para la nueva red lógica se propone utilizar la misma infraestructura que posee la empresa actualmente y ampliar los puntos de datos de 13 a 16 puntos, esto con el fin de tener alguna contingencia por la aparición de un nuevo puesto o cargo o también para el caso de que se decida colocar una impresora o algún otro dispositivo de red.

- Red LAN

La topología se mantendrá igual, es decir, se continúa usando la red tipo estrella soportada en los switches y el concentrador actuales.

- Protocolo

De igual forma que la red LAN también se mantendrá el protocolo de TCP/IP en su versión 4 que se venía usando. El rango de direcciones será el mismo, pero usando los servicios de DHCP del servidor de Windows 2003 Server se asignarán automáticamente las direcciones a los equipos que se conecten a la red de la siguiente forma:

- Rango de direcciones: 192.168.0.100 – 192.168.0.120
- Máscara de subred: 255.255.255.0
- Puerta de enlace: 192.168.0.1
- Direcciones reservadas: 192.168.0.1 – 192.168.0.10
- DNS's: Los asignados por el ISP

- Conexión a Internet

Se realizará un nuevo acuerdo con el proveedor Telecom para que ofrezca las siguientes características al servicio:

- Velocidad: 384 kbps
- Reuso: 1:1
- Calidad de servicio: 60 kbps reservados para dos llamadas por IP
- Filtro de antivirus y spam en el lado de su enrutador

- Conexión VPN

La conexión VPN para la comunicación de datos entre las dos sedes se realizará a través de un firewall *3COM® OfficeConnect® VPN Firewall*, el cual además de brindar una conexión segura y confiable entre las sedes brindará los servicios de:

- Filtro web
- Detección de intrusos y ataques
- Reportes de uso de canal
- Accesos no autorizados a la red interna
- Permite dar prioridad al tráfico en Internet garantizado ancho de banda deseado para voz y multimedia
- Permite usar DHCP para establecer las direcciones de red de los equipos internos
- Acceso compartido y seguro a Internet

Ver hoja de datos [3COM® OfficeConnect® VPN Firewall](#)

Se deberá instalar uno en Cartagena y otro en Valledupar.

- Correo electrónico

Luego de la gestión del dominio www.autobol.com por parte de la empresa Telecom se solicitará la cesión de la administración de la cuenta, esto con el fin de que Autobol S.A. se entienda directamente con la empresa a la que se le arrienda el derecho de uso de este y así evitar posibles futuros inconvenientes si desea cambiar de ISP.

Se utilizará un servidor en cada sede (Cartagena y Valledupar), para proveer cuentas de correo electrónico a través de Microsoft Exchange, cada responsable de departamento, área o proceso de Autobol S.A. determinará quienes de las personas que están a su cargo deberán tener una cuenta de correo electrónico de la compañía para el ejercicio de sus funciones y solicitará

al departamento de sistemas de la sede correspondiente la creación de la respectiva cuenta.

Sede en Valledupar

- Red lógica

Se propone habilitar 14 puntos de red. Distribuidos de la siguiente manera:

- 1 punto para Gerente General
- 1 Punto para secretaria de Gerencia
- 1 Asistente de Ventas
- 1 Secretaria de Ventas
- 2 Almacen de repuestos
- 1 Servidor
- 1 Administrador de Sistemas
- 1 Secretaria de taller
- 1 Cobtabilidad
- 1 Secretaria de contabilidad
- 1 caja
- 2 puntos de contingencia

- Red LAN

La topología de red a utilizar es tipo estrella soportada en un Switch.

- Protocolo

Protocolo de TCP/IP en su versión 4. Se usaran los servicios de DHCP del servidor de Windows 2003 Server se asignarán automáticamente las direcciones a los equipos que se conecten a la red de la siguiente forma:

- Rango de direcciones: 192.168.0.130 – 192.168.0.150

- Máscara de subred: 255.255.255.0
- Puerta de enlace: 192.168.0.2
- Direcciones reservadas: 192.168.0.11 – 192.168.0.20
- DNS's: Los asignados por el ISP

- Conexión a Internet

Se contratará un proveedor de servicio de Internet, que brinde un servicio con las siguientes características:

- Velocidad: 384 kbps
- Reuso: 1:1
- Calidad de servicio: 60 kbps reservados para dos llamadas por IP
- Filtro de antivirus y spam en el lado de su enrutador

- Conexión VPN

La conexión VPN para la comunicación de datos entre las dos sedes se realizará a través de un firewall *3COM® OfficeConnect® VPN Firewall*, el cual además de brindar una conexión segura y confiable entre las sedes brindará los servicios de:

- Filtro web
- Detección de intrusos y ataques
- Reportes de uso de canal
- Accesos no autorizados a la red interna
- Permite dar prioridad al tráfico en Internet garantizado ancho de banda deseado para voz y multimedia
- Permite usar DHCP para establecer las direcciones de red de los equipos internos
- Acceso compartido y seguro a Internet

Ver hoja de datos [*3COM® OfficeConnect® VPN Firewall*](#)

Hardware

Para la oficina de Cartagena se mantendrá el mismo hardware con la excepción de las nuevas adquisiciones, entre las cuales tenemos el nuevo Firewall y el nuevo servidor para la centralización de la información de las dos sedes.

El servidor tendrá las siguientes especificaciones:

- SO Windows 2003 Server
- Procesador Intel® Xeon® 3070 2.66 GHz
- Controladora SCSI Raid 5
- 3 Discos Duros de 36.2 GB de 15krpm
- 4 GB de memoria RAM
- Unidad Óptica DVD ROM
- Unidad Interna LTO Ultrium Generation 2 (200/400 GB)
- Red 10/100/1000 Mbps

Para la oficina de Valledupar se comprarán los siguientes equipos descritos a continuación:

- Un servidor así:
 - SO Windows 2003 Server
 - Procesador Intel® Xeon® 3040 1.86 GHz
 - Controladora SCSI Raid 5
 - 3 Discos Duros de 18.1 GB de 15krpm
 - 2 GB de memoria RAM
 - Unidad Óptica DVD ROM
 - Unidad Interna LTO Ultrium Generation 1 (100/200 GB)
 - Red 10/100/1000 Mbps

- Nueve estaciones de trabajo así:
 - SO Windows XP Professional SP 2

- Procesador Intel® Core™ 2 Duo E6300 1.86 GHz
 - Disco duro de 60 GB
 - 1 GB de memoria RAM
 - Unidad Óptica DVD ROM
 - Red 10/100 Mbps
- Un Wireless Access Point
 - Dos computadores portátiles así:
 - SO Windows XP Professional SP 2
 - Procesador Intel® Core™ 2 Duo T7200 2.00 GHz
 - Disco duro de 60 GB de 5400 rpm
 - 1 GB de memoria RAM
 - Unidad Óptica DVD ROM
 - Red 10/100 Mbps
 - Wi-fi
 - Una impresora láser multifuncional que permita:
 - Impresión en red
 - Envío de fax
 - Escaneo
 - Dos impresoras de matriz de punto
 - Cableado estructurado de voz y datos categoría 5e
 - Un switch ethernet de 24 puertos así:
 - Administrable vía web
 - Chasis para montaje en rack
 - Conexión Gigabit a servidores
 - Una UPS central de 2 KVA
 - 1 equipo de computo analizador de gases
 - 1 equipo de computo para alineación
 - 1 equipo de computo diagnosticador de fallas

6.2.3.3. Políticas de sistemas

Las políticas generales para el área de Sistemas serán:

- Elaborar anualmente un plan de contingencias para el área de Sistemas con el fin de tener una guía a seguir en el momento que se presente una eventualidad con cualquiera de los sistemas de información de la compañía.
- Todo el software utilizado en la compañía deberá estar respaldado por su respectiva licencia.
- Se mantendrá el hardware y el software actualizados de tal manera que permitan cumplir con el normal desarrollo de las actividades de la compañía.

6.2.3.4. Política de seguridad y control informático

Es primordial para Autobol S.A. preservar sus activos de información de propiedad de la compañía y permitir su utilización, acceso y divulgación de acuerdo exclusivamente con los intereses de la compañía o los requerimientos de las autoridades competentes. La información de propiedad de Autobol S.A. está sólo para disposición de personal autorizado de Autobol S.A. basándose en la necesidad de su utilización para el ejercicio de las actividades de la compañía. Los recursos informáticos de Autobol S.A. usados para almacenar, procesar y distribuir la información de propiedad deberán ser administrados, controlados, y resguardados siguiendo esta política. Además, el uso de los recursos computacionales de la compañía que incluyen el hardware y el software para cualquier actividad que no pertenezca a la compañía, incluyendo el uso personal, está prohibido a menos que este sea previamente aprobado.

Responsabilidades

Todos los empleados de Autobol S.A. y empleados temporales que estén autorizados para utilizar los recursos informáticos y de red de la compañía deberán reconocer que tienen responsabilidades en relación con la seguridad de estos activos. Los asesores, analistas, jefes e ingenieros son algunos de los cargos o funciones que tienen responsabilidades además de todas aquellas que se aplican a los usuarios generales.

Las siguientes son las responsabilidades de los usuarios:

- Garantizar que los datos de la compañía que se encuentren bajo su control estén debidamente identificados y resguardados según su clasificación de propiedad conforme con las políticas de la compañía.
- Cumplir con las prácticas de seguridad y protección.
- Usar los recursos informáticos y de red sólo cuando estén autorizados y solo para fines aprobados.

Información propietaria

Visión General

Para Autobol S.A. la información es un activo y de acuerdo a su uso puede ser valorada tanto como el equipo, la propiedad o el efectivo. Por este motivo se han elaborado unas políticas y requerimientos de seguridad para salvaguardar este activo.

Debido al propósito de estas políticas, "información de Propiedad" es toda información tangible o intangible: creada, obtenida o controlada por la compañía que no haya sido entregada a otros sin restricción y que la compañía desee mantener como confidencial.

También se considera de propiedad la información de otros la cual haya sido obligada a guardar como confidencial.

Ejemplos de información propietaria

La información propietaria incluye varios tipos de información, entre los que se incluyen: comercial, financiera, técnica y confidencial. Normalmente la información propietaria puede incluir: registros de contabilidad, planos de construcciones, planos, software, diagramas, material de capacitaciones, estrategias de ventas, informes de costos, listas de precios, registros de clientes, análisis de riesgos, entre otros. Datos que si se dan a conocer al público o la competencia causarían daño importante a Autobol S.A.

Políticas de información propietaria

Es para Autobol S.A. una política salvaguardar sus activos de información propietaria y compartirlos con otras personas solo cuando sea de interés de Autobol S.A. hacerlo y que esta revelación no infrinja las leyes o esté legalmente prohibida.

La información propietaria de Autobol S.A. debe ser resguardada en todo momento por todo el personal de la compañía. Su utilización o divulgación no autorizada podría:

- Destruir su valor para Autobol S.A.
- Impactar la privacidad del cliente, proveedor o empleado.
- Reducir la competitividad de la compañía.
- Facilitar una ventaja desigual a otros.

Por todo lo anterior todo el personal de Autobol S.A. debe cumplir con estas normativas.

Controles de acceso a información propietaria

El creador o propietario y los receptores de información propietaria de Autobol S.A. deberán saber como salvaguardar la información cuando esta se encuentre bajo su poder.

Copia de información propietaria

La información propietaria de Autobol S.A. podrá ser copiada para su posterior distribución por cualquier empleado de Autobol S.A. que tenga necesidad de conocer con una razón comercial para hacerlo.

La información propietaria restringida de Autobol S.A. solo podrá ser copiada por el creador o propietario y los receptores autorizados por el creador o propietario.

Responsabilidades sobre información propietaria

Todos los empleados de Autobol S.A. son responsables de proteger la información propietaria en su poder de acuerdo con los requerimientos contenidos en este documento. Si son receptores de información propietaria, entonces deben:

- No divulgar o debatir el contenido, a menos que sea aprobado conforme a las restricciones asociadas en su clasificación.
- Conservarla segura en todo momento.
- No divulgarla a personal extraño a Autobol S.A., excepto si hay necesidad de conocerla y previa firma a un acuerdo de no revelación.
- Notificar al departamento administrativo de Autobol S.A., si existen razones que indiquen que información propietaria puede ser o ha sido robada, perdida o de otra forma no se ha localizado.

Todos los jefes son responsables de:

- Garantizar que todas las personas a su cargo (empleadas o por contrato) conocen y cumplen los requerimientos de seguridad para la protección de la información propietaria.
- Recordar a las personas a su cargo sus compromisos de no divulgación, de devolver todos los documentos que contengan información propietaria de la compañía (como reportes, impresiones, discos compactos, fotografías, películas).

- Hacer seguimiento de la partida de un empleado para asegurar que este no tome información propietaria.

Los trabajadores por contrato o temporales son responsables de resguardar la información propietaria de Autobol S.A. y deben:

- Firmar acuerdos de no revelación y/o el acuerdo correspondiente a propiedad intelectual.

Computación general

Autenticación

La autenticación concierne al proceso de probar una identidad para la satisfacción de alguna autoridad que da un permiso. Los sistemas de autenticación son hardware y/o software y/o procedimientos que permiten que un usuario acceda a los recursos informáticos y de red de una compañía.

Complejidad de contraseñas

Cuando el método de autenticación es la contraseña, el sistema debe ser configurado para que cuando se creen o se cambien no se permita que se haga en forma trivial y siguiendo los siguientes parámetros:

- Las contraseñas deben tener un mínimo de 6 (seis) caracteres alfanuméricos.
- La elaboración de la contraseña debe ser lo suficientemente compleja con el fin de evitar que se puedan establecer como contraseñas datos como: nombres, fechas, palabras del diccionario, números telefónicos, etc.
- No permitir el uso de contraseñas nulas o en blanco.

Asignación de identificadores de usuarios

Se deben asignar identificadores de usuarios únicos a los empleados y estos no deben ser compartidos, con el fin de proveer la capacidad de realizar auditorias sobre movimientos o transacciones realizadas por los usuarios.

Protección de las contraseñas de administrador

Debe existir un procedimiento que permita garantizar la seguridad y el control de las contraseñas de administrador.

Deshabilitación de identificadores inactivos

Todos los identificadores de usuarios que no hayan sido utilizados por más de 45 días consecutivos serán deshabilitados y no reactivados hasta que un jefe de departamento haga la respectiva solicitud.

Eliminación de identificadores

Todos los identificadores de usuarios que no hayan sido usados por más de 120 días serán eliminados del sistema.

Validación anual de identificadores de empleados

El administrador del sistema revisará todos los identificadores asociados a los empleados de la compañía y determinará verificando con los jefes de departamento si los permisos y comandos asociados a los identificadores son los apropiados de acuerdo del trabajo de los usuarios. Se hará cualquier cambio necesario en este proceso.

Expiración de contraseñas

Las contraseñas pre-asignadas o temporales deben ser forzadas a que sean cambiadas por el usuario en el primer acceso al sistema por parte del usuario. Por otra parte se debe configurar el sistema para que este exija al usuario que cambie de contraseña cada 45 días, con avisos previos a la fecha de vencimiento con 10 días de anterioridad.

Cambio de contraseñas del sistema

Las contraseñas del sistema se deben cambiar inmediatamente si estas han sido conocidas por terceros, de lo contrario cada 45 días por lo menos o si son de usuarios privilegiados cada 30 días.

Reutilización de contraseñas

El sistema debe ser configurado para que no permita la utilización de las ultimas 6 (seis) claves usadas por los usuarios.

7. CONCLUSIONES

El MSV [1] es una metodología que puede ser usada en muchos ámbitos organizacionales ya que por su facilidad para ser interpretada permite analizar cualquier proceso de una organización para darle continuidad, cambio o detenimiento en un momento determinado. El MSV permite analizar los procesos de la organización desde puntos de vista internos y externos con el fin de visualizar como se están llevando estos actualmente y los posibles futuros escenarios de los mismos. Como también ejercer supervisión y coordinación entre los mismos procesos.

Otra herramienta que se utilizó fue el modelo COSO [5], que permite, a partir de los componentes del sistema de control interno, hacer análisis de la situación actual de la organización, identificar fallas y crear mecanismos de control con el fin de hacer monitoreo y seguimiento a los procesos.

Las dos herramientas fueron de utilidad porque contribuyeron al diseño de las tres etapas que contempla el modelo propuesto.

Continuando con este trabajo se podría realizar el análisis para la implementación en la compañía Autobol S.A. lo siguiente:

- La elaboración de un plan de contingencias para el área de Sistemas.
- Revisión y actualización de las políticas de sistemas propuestas en este trabajo.

Lo anterior, tiene relación con el modelo propuesto en este trabajo dado que tanto COSO como el MSV sugieren el seguimiento y monitoreo de las medidas de control implementadas, con el fin de adaptarlas a los cambios que se van presentando y para aplicar labores de mejora continua.

8. BIBLIOGRAFÍA

- [1] Espejo, R. (2003) "The Viable System Model A Briefing About Organisational Structure",
<http://syncho.com/pages/pdf/INTRODUCTION%20TO%20THE%20VIABLE%20SYSTEM%20MODEL3.pdf>, Julio 2007
- [2] Suárez, C. <http://www.monografias.com/trabajos7/gepla/gepla.shtml>, Julio 2007
- [3] <http://www.monografias.com/trabajos32/sistema-viable/sistema-viable.shtml>
- [4] <http://www.coso.org/>, Julio 2007
- [5] Ladino, E. <http://www.monografias.com/trabajos12/coso/coso.shtml>, Julio 2007
- [6] http://controlinterno.udea.edu.co/ciup/nuevo_sci.htm, última modificación: 11 de Octubre de 2006, Julio 2007
- [7] Coopers & Lybrand e Instituto de Auditores Internos de España (1997) "Los Nuevos Conceptos de Control Interno (Informe COSO)
- [8] Pérez, P.
http://www.degerencia.com/articulo/los_cinco_componentes_del_control_interno,
Julio 2007
- [9] <http://www.funcionpublica.gob.mx/scagp/ucegp>, Julio 2007
- [10] <http://www.definicion.org/vision>, Julio 2007
- [11] Codina, A. <http://www.degerencia.com/articulos.php?artid=644>, Julio 2007
- [12] <http://www.grupoconsultoria.com.co>, Julio 2007