ESCUELA POLITÉCNICA DEL EJÉRCITO

DPTO. DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

PLANIFICACIÓN ESTRATÉGICA Y PLAN DE SEGURIDAD INFORMÁTICA DE FABRIL FAME S.A.

Previa a la obtención del Título de:

INGENIERO EN SISTEMAS E INFORMÁTICA

DIRECTOR: INGENIERO MARIO RON
CODIRECTOR: INGENIERO VÍCTOR PÁLIZ

POR: JOSÉ LUIS ROJAS URGILÉS
JUAN JOSÉ VELA VEINTIMILLA

SANGOLQUÍ, 9 de NOVIEMBRE de 2011

CERTIFICACIÓN

Certifico que el presente trabajo fue realizado en su totalidad por los Señores José Luis Rojas Urgilés y Juan José Vela Veintimilla, candidatos a Ingenieros como requerimiento parcial a la obtención del título de Ingenieros en Sistemas e Informática.

Sangolquí, 9 de Noviembre 2011

Ing. Mario Ron	**Ing. Víctor Páliz**
DIRECTOR	**CO - DIRECTOR**

DEDICATORIA

Primero a Dios, a mi Madre Dolorosa, a mis padres Luis y Patricia, a Susy, a mis hermanas Verónica, Carolina y Cinthya, a mi sobrino Gabriel, a mis abuelitos Inés y Carlos, Consuelito y Leonidas; a mis tíos y a toda mi familia, a mis amigos Felipe, Anderson, Juanjo, Batros, etc., y a todos los que creyeron en mí, por sus consejos y su apoyo a lo largo de mi vida.

JOSÉ LUIS ROJAS

Este proyecto de tesis está dedicado a mis padres, a mi abuelita, a mi hermana y familia, a mi novia Maritza, y a mi familia en general; a mis ñaños los Bao´s, a mis mejores amigos del colegio y universidad y a todos aquellos que han estado en este y otros proyectos de mi vida.

JUAN JOSÉ VELA

AGRADECIMIENTO

A Dios y a la Dolorosa por su infinito amor y todas las bendiciones recibidas a lo largo de mi vida, a mis padres Luis y Patricia por su apoyo incondicional.

Al Ing. Mario Ron, Mauricio Campaña, Víctor Páliz y a todos los profesores a lo largo de la carrera universitaria, por ser la guía con sus amplios conocimientos y consejos, a lo largo de todo el desarrollo de este proyecto y de nuestra carrera politécnica.

A toda mi familia, amigos y a los que creyeron en mí.

JOSÉ LUIS ROJAS

Agradezco a Dios por haberme permitido lograr este objetivo, a mis padres por su apoyo incondicional, a mi hermana y familia por siempre alentarme a lograrlo, a mi novia Maritza por estar conmigo, incentivando mi crecimiento profesional e incluso ayudándome con este proyecto, a mis amigos y hermanos por el reconocido dicho "Que será de la tesis", a todos muchas gracias ya que con sus consejos, pude lograrlo.

A todos los profesores que tuve durante la carrera por su amplio conocimiento y su entrega a la enseñanza, a los ingenieros: Mario Ron, Víctor Páliz y Mauricio Campaña por ser mi guía para este y muchos otros proyectos presentados durante la carrera.

JUAN JOSÉ VELA

íNDICE

ÍNDICE TABLAS

ÍNDICE DIAGRAMAS

RESUMEN

El presente proyecto pretende obtener como producto final la Planificación Estratégica y Plan de Seguridad informática para el Departamento de Sistemas de la empresa Fabril FAME S.A.

Mediante El Plan Estratégico Informático se gestiona el uso de la Información y se planifica la implementación de los sistemas informáticos que resuelvan las necesidades específicas de la empresa. En este proyecto se refleja una visión de alto nivel de los requerimientos de información de la organización FAME S.A., y se desarrolla una planificación para satisfacer dichos requerimientos mediante el levantamiento de información a los usuarios en las áreas de los procesos claves, a través de entrevistas y observación.

Para este desarrollo se aplica la metodología PETI (Planificación Estratégica de Tecnologías de Información), que permite el entendimiento administrativo de la empresa para desarrollar las estrategias de tecnologías de información que impulsen las estrategias de negocio.

Se ha identificado las falencias existentes y puntos críticos de la organización y se ha planteado soluciones tecnológicas para reducir el impacto de estas falencias y que impulsen a FAME S.A. en la consecución de sus objetivos empresariales.

El Plan de Seguridad Informática constituye el documento básico que establece los principios organizativos y funcionales de la actividad de Seguridad Informática en una Entidad y recoge claramente las políticas de seguridad y las responsabilidades de cada uno de los participantes en el proceso informático, así como las medidas y procedimientos que permitan prevenir, detectar y responder a las amenazas que existen.

En el presente proyecto, previo a la elaboración del documento de política de seguridad se desarrollo un análisis de riesgos que es el proceso cuantitativo o cualitativo que permite evaluar los riesgos; determina cómo es, cuánto vale, cómo y cuan protegidos se encuentran los activos, en coordinación con los objetivos, estrategia y política de la organización.

Para la elaboración del análisis de riesgos se utilizaron la metodología y herramienta MAGERIT 2.0 y PILAR 5.1 respectivamente, gracias a estos se pudo obtener resultados con los cuales se puede medir el grado de seguridad de la información que actualmente tiene la empresa.

Las actividades de gestión de los riesgos detectados permitieron elaborar un plan de seguridad que satisfaga todas las necesidades de empresa. El desarrollo del plan fue basado en la norma ISO/IEC 27002 que es una guía de buenas prácticas y recomendaciones a seguir para implementar salvaguardas o seguridades de información.

CAPÍTULO I

INTRODUCCIÓN

1.1.- TEMA

Planificación Estratégica y Seguridad Informática del departamento de sistemas de la empresa Fabril Fame S.A.

1.2.- DESCRIPCIÓN DE LA EMPRESA

FABRIL FAME S.A., es una prestigiosa empresa reconocida a nivel nacional, dentro de la industria textil del Ecuador, gracias a sus procesos de producción de calidad. Además pertenece al grupo HOLDING DINE S.A., una corporación industrial y comercial que ha implementado varios procesos de alta competitividad que le han valido para obtener prestigiosos reconocimientos y posicionamiento en el competitivo mercado ecuatoriano.

1.3.- PLANTEAMIENTO DEL PROBLEMA

La empresa FAME, tiene la responsabilidad de fomentar una infraestructura informática planificada que le permita mantener sus sistemas de información siempre en línea, con un Departamento de Sistemas, que pueda atender y solucionar todos lo requerimientos de la empresa, como son:

- Administración general de la red y sus recursos
- Capacitación a los usuarios
- Seguridades y Control

- Actualización y Desarrollo
- Soporte a usuarios
- Mantenimiento de los Sistemas Informáticos

Debido a las exigencias informáticas cotidianas de la empresa, el Departamento de Sistemas ha dejado pasar por alto la definición de la planificación informática a mediano o largo plazo, que le permita tener un claro horizonte de desarrollo, asegurando así, la asignación de recursos correspondientes para lograr sus metas.

Por otra, parte el Departamento de Sistemas no tiene definidas políticas informáticas que aseguren la integridad, confidencialidad, confiabilidad y oportunidad, de su información, además, se hace necesario planes de contingencia que permitan actuar y superar inesperados inconvenientes en sus sistemas de información.

1.4.- JUSTIFICACIÓN

Planificar significa estudiar anticipadamente los objetivos y acciones, que permitan sustentar los actos no en corazonadas sino con algún método, plan o lógica. Los planes establecen los objetivos de la organización y definen los procedimientos adecuados para alcanzarlos.

Además los planes son la base fundamental para que una organización como FAME, obtenga y aplique los recursos para lograr sus objetivos; además para que los miembros de la organización desempeñen actividades y tomen decisiones congruentes con los objetivos y procedimientos escogidos, ya que enfoca la atención de los empleados sobre los objetivos que generan resultados, por otro lado, controla el logro de los objetivos organizacionales. Asimismo, ayuda a fijar prioridades;

permite concentrarse en las fortalezas de la organización, ayuda a tratar los problemas de cambios en el entorno externo entre otros aspectos.

La existencia de personas ajenas a la información, también conocidas como piratas informáticos o hackers, que buscan tener acceso a la red empresarial para modificar, sustraer o borrar datos, son una amenaza latente para cualquier institución

Tales personajes pueden, incluso, formar parte del personal administrativo o de sistemas, de cualquier compañía; de acuerdo con expertos en el área, más de 70 por ciento de las violaciones e intrusiones a los recursos informáticos se realiza por el personal interno, debido a que éste conoce los procesos, metodologías y tiene acceso a la información sensible de su empresa, es decir, a todos aquellos datos cuya pérdida puede afectar el buen funcionamiento de la organización.

Esta situación se presenta gracias a los esquemas ineficientes de seguridad con los que cuentan la mayoría de las compañías a nivel mundial, y porque no existe conocimiento relacionado con la planeación de un esquema de seguridad eficiente que proteja los recursos informáticos de las actuales amenazas combinadas.

El resultado es la violación de los sistemas, provocando la pérdida o modificación de los datos sensibles de la organización, lo que puede representar un daño con valor de miles o millones de dólares.

Contar con un plan definido de estrategias, procedimientos y seguridades informáticas, le brindarán herramientas eficaces a FAME para actuar frente a varias amenazas y eventualidades que puedan poner en riesgo la integridad de su información, así como contar con los recursos necesarios para mantener de manera adecuada la infraestructura informática y poder reaccionar técnicamente a las diversas necesidades cotidianas de la empresa.

1.5.- OBJETIVOS GENERAL Y ESPECÍFICOS

1.5.1.- General

Desarrollar un Plan Estratégico y de Seguridad Informática, para proteger los recursos informáticos y asegurar la viabilidad de las operaciones de la empresa Fabril Fame S.A.

1.5.2.- Específicos

- Analizar los procesos actuales que maneja el Departamento de Sistemas de FAME
- Determinar la estrategia general de tecnología informática para ser implementada en la institución.
- Determinar el acceso a la información de acuerdo a los niveles de seguridad y perfiles de usuario.
- Elaborar el análisis de riesgos de los sistemas de información de FAME.
- Establecer políticas de seguridad física, lógica y comunicaciones de FAME, dentro del Plan de Seguridad Informática.
- Ajustar y optimizar los procesos actuales de tecnología.
- Mejorar la eficiencia del Departamento de Sistemas, frente a las diferentes situaciones y necesidades de la empresa, en el ámbito informático.
- Optimizar y explotar el uso de recursos tecnológicos de FAME, para su máximo provecho.

1.6.- ALCANCE DEL PROYECTO

El resultado del proyecto será el Plan estratégico del Departamento de Sistemas y el Plan de Seguridad Informática, los que incluirán:

- La identificación de los procesos en tecnologías de información.
- La elaboración del plan de procedimientos a corto plazo y calendario de trabajo en el periodo de tiempo estimado.
- La clasificación de la información en niveles de importancia.
- Planteamientos de seguridad física, lógica y de comunicaciones.

El Plan Estratégico y de Seguridades Informáticas deberá constituir una herramienta, permanentemente, para la mejora en los procesos administrativos y tecnológicos de la empresa FAME, optimizando la función informática, el conjunto de la organización y los métodos utilizados, y estableciendo las líneas estratégicas para los sistemas, con objeto de dar un soporte ágil y eficiente a las necesidades evolutivas de las distintas áreas de la empresa. Además permitirá salva guardar la integridad de la información, evitando perdida de la misma o acceso por entes no autorizados.

CAPÍTULO II

MARCO TEÓRICO DE REFERENCIA

2.1.- CONCEPTOS DE PLANIFICACIÓN INFORMÁTICA

2.1.1.- Definición de Planificación Estratégica Informática

La planificación es prever y decidir hoy las acciones que pueden llevar desde el presente hasta un futuro deseable. No se trata de hacer predicciones acerca del futuro sino de tomar las decisiones pertinentes para que ese futuro ocurra. La planificación es un proceso gradual, por el cual se establece el esfuerzo necesario para cumplir con los objetivos de un proyecto. Este proceso permite además, refinar los objetivos que dieron origen al proyecto.

Existen diferentes herramientas y técnicas para abordar la planificación de un proyecto, las cuales permiten definir el curso de acción a seguir, que será tomado como base durante la ejecución del mismo. Si bien la planificación define las acciones a seguir, durante la ejecución puede existir necesidad de cambios respecto de lo definido originalmente, los mismos servirán de punto de partida para un nuevo análisis y una nueva planificación de ser requerido.

- Planificación de corto plazo: el período que cubre es de un año.
- Planificación de mediano plazo: el período que cubre es más de un año y menos de cinco.
- Planificación de largo plazo: el período que cubre es de más de cinco años.

La estrategia es el conjunto de decisiones y criterios por los cuales una organización se orienta hacia el logro de sus objetivos. Es decir, involucra su propósito general y establece un marco conceptual básico por medio del cual, ésta se transforma y se adapta al dinámico medio en que se encuentra inserta.

Entonces, planificación estratégica informática, es el proceso de estudiar, analizar y decidir las mejores estrategias de incorporación y uso de los sistemas informáticos (SI) y de las TIC (tecnologías de la información y de telecomunicaciones) en una organización; es decir define los caminos a seguir en un cierto periodo de tiempo futuro, en forma perfectamente alineada con la misión y objetivos de la organización.

La planificación estratégica de sistemas de información intenta identificar y establecer prioridades acerca de la tecnología y aplicaciones susceptibles de reportar un máximo beneficio a la empresa.

Un plan estratégico de sistemas de información indica la dirección correcta en el desarrollo de los sistemas de información, el modo de proceder, los criterios de selección, mecanismos de evaluación, etc.

2.1.2.- Importancia de la Planificación Estratégica Informática

Planificar significa que los ejecutivos estudian anticipadamente sus objetivos y acciones, y sustentan sus actos no en corazonadas sino con algún método, plan o lógica. Los planes establecen los objetivos de la organización y definen los procedimientos adecuados para alcanzarlos.

Además los planes son la guía para que la organización obtenga y aplique los recursos para lograr los objetivos; los miembros de la organización desempeñen

actividades y tomen decisiones congruentes con los objetivos y procedimientos escogidos, ya que enfoca la atención de los empleados sobre los objetivos que generan resultados pueda controlarse el logro de los objetivos organizacionales.

Asimismo, ayuda a fijar prioridades, permite concentrarse en las fortalezas de la organización, ayuda a tratar los problemas de cambios en el entorno externo, entre otros aspectos.

Por otro lado, existen varias fuerzas que pueden afectar a la planificación: los eventos inesperados, la resistencia psicológica al cambio ya que ésta acelera el cambio y la inquietud, la existencia de insuficiente información, la falta de habilidad en la utilización de los métodos de planificación, los elevados gastos que implica, entre otros.

Las decisiones sobre qué hacer en el futuro con los sistemas de información en las organizaciones generalmente han pasado por cuatro etapas. La primera coincide con la aparición de la informática en las organizaciones durante la década de los 70's. En este punto, las aplicaciones informáticas afectaban principalmente a los departamentos de contabilidad y de facturación, por su fácil implementación. Durante esta etapa siempre se desarrollaba un nuevo sistema de información cuando un departamento lo solicitaba, por lo que no existía un plan estratégico de sistemas de información.

La segunda etapa se caracterizaba por el aumento indiscriminado de peticiones por parte de los usuarios. Además de solicitar cada vez más aplicaciones informáticas, los problemas eran cada vez más complejos. Debido a las limitaciones en recursos por parte de los departamentos de sistemas, era necesario definir criterios de selección y priorización. Sin embargo, estos criterios no eran coherentes

con los objetivos estratégicos de la empresa, sino con el poder de los usuarios que lo habían solicitado o con el atractivo del proyecto.

La asignación de recursos para el desarrollo de proyectos en función de los objetivos estratégicos de la organización es la característica de la tercera etapa. Los altos directivos de la organización definen los criterios para identificar y priorizar dichos proyectos para el desarrollo de sistemas informáticos según los objetivos de la organización. Es por este motivo que se le denomina plan estratégico de sistemas de información, en función de la estrategia de la organización. Otro aspecto que se introduce en esta etapa es la definición de una infraestructura común para todos los desarrollos de sistemas informáticos.

La cuarta etapa es conocida como la interdependencia estratégica de la empresa con los sistemas de información. Para conseguirlo, los responsables de la organización deben integrar las posibilidades de los SI, con la estrategia de la empresa en el momento de su formulación, y no después, tal y como ocurría en la tercera etapa. Esta tarea es muy difícil tal y como muestra el reducido número de organizaciones que se encuentran en esta situación, ya que, es necesaria una cultura organizativa sensible al potencial de la tecnología.

Es necesario inculcar una cultura que permita implementar una metodología activa, es decir, una metodología en donde la definición de objetivos estratégicos tenga en cuenta las posibilidades de las tecnologías de la información.

2.2.- METODOLOGÍA DE LA PLANIFICACIÓN ESTRATÉGICA PETI

La metodología PETI (Planeación Estratégica de Tecnología de Información) es ampliamente reconocida como una herramienta para ordenar los esfuerzos de incorporación de TI.

Establece las políticas requeridas para controlar la adquisición, el uso y la administración de los recursos de TI. Integra la perspectiva de negocios/organizacional con el enfoque de TI, estableciendo un desarrollo informático que responde a las necesidades de la organización y contribuye al éxito de la empresa. Su desarrollo está relacionado con la creación de un plan de transformación, que va del estado actual en que se encuentra la organización, a su estado final esperado de automatización, esto, en concordancia con la estrategia de negocios y con el propósito de crear una ventaja competitiva.

La PETI consiste en un proceso de planeación dinámico, en el que las estrategias sufren una continua adaptación, innovación y cambio, que se refleja en los elementos funcionales que componen toda la organización. Trabajos relacionados con la construcción de un PETI, han sido desarrollados desde hace tres décadas, pero presentan limitaciones importantes.

La metodología de PETI (tabla 2.1), correspondiente a la categoría de metodologías integrales, que consta de quince módulos agrupados en cuatro fases. Este paradigma está concebido, en concordancia con el modelo conceptual, a través de una visión estratégica de negocios/organizacional y una visión estratégica de TI. La metodología integra ambas visiones en una única final.

Tabla 2.1: Metodología de Planeación Estratégica de Tecnología de Información

		Módulos PETI
FASE 1	Situación Actual	Análisis de Situación
FASE 2	Modelo de Negocios/Organización	Análisis de Entorno Estrategia de Negocios Modelo Operativo Estructura de la Organización Arquitectura de la Información
FASE 3	Modelo de TI	Estrategia de TI Arquitectura de SI Arquitectura Tecnológica Modelo Operativo TI Estructura Organizacional TI
FASE 4	Modelo de Planeación	Prioridades de Implantación Plan de Implantación Recuperación de la Inversión Administración del riesgo

2.2.1.- Situación Actual

2.2.1.1.- Análisis de Situación

El proceso comienza con un análisis de la situación actual en la fase I, que produce el modelo funcional imperante en la empresa. Involucra un examen y estudio del estado actual de la empresa. Produce como resultado el modelo funcional en el que opera la organización. El propósito es entender apropiadamente la posición de la empresa, sus problemas y madurez tecnológica.

Esta fase cuenta con un solo módulo: análisis de la situación actual, que se divide en dos pasos.

El primero trata sobre la identificación del alcance competitivo de la organización. Establece las características principales que influyen en la estrategia de negocios, y describe el comportamiento global de la empresa.

El segundo paso está relacionado con una evaluación de las condiciones actuales de la empresa. Dicha revisión debe incluir la evaluación de tres aspectos fundamentales: estrategias de negocios, modelo operativo y TI. Este esfuerzo se encarga de desarrollar el entendimiento de alto nivel de la situación actual de la empresa.

El paso relacionado con la estrategia de negocios, se enfoca a la revisión del conocimiento actual sobre la organización en planeación estratégica. No debe confundirse con el establecimiento de las estrategias. De hecho está relacionado con el entendimiento de alto nivel sobre la estrategia de la organización; la difusión a ejecutivos altos y medios, y la manera como éstos se involucran con el plan estratégico de la organización. El modelo operativo consiste en una revisión y el estudio de las condiciones en que se encuentran las áreas funcionales. Los procesos y las actividades deben ser identificados, evaluados y asociados con la información requerida por cada área. Los datos deben ser obtenidos con base en la observación, así como a través de entrevistas con ejecutivos y usuarios clave. El propósito es determinar la situación del entorno en la organización, identificar problemas y establecer las necesidades de información dentro y fuera de la función informática. El análisis debe concentrarse en el entendimiento de la operación, sin necesidad de considerar la estructura de la organización.

El paso de TI trata con la evaluación de:

- Las capacidades del portafolio de aplicaciones de software e infraestructura técnica (hardware y comunicaciones), identificando debilidades y deficiencias tecnológicas.
- La conformación de la estructura de la organización de TI (recursos humanos), que consiste en el examen de la capacidad de los recursos humanos y la conformación de la estructura de puestos del personal.
- El análisis financiero, relacionado con la inversión histórica y actual en TI, y el retorno de la inversión esperada. Este punto busca inspeccionar los estándares de inversión de la empresa y compararlos ("benchmarketing") con los estándares de inversión del mercado, justificando la situación informática actual.

Es importante notar que esta reseña no debe ser demasiado detallada y es conveniente llevarla a cabo en un tiempo corto. El detalle del modelo deberá ser alcanzado en las fases subsecuentes

2.2.2.- Modelo de Negocios/Organización

En esta fase la metodología está relacionada con la creación de un modelo de negocios/organización, que representa la piedra fundamental del proceso de planeación de TI. Se concentra en el entendimiento del entorno y el establecimiento de la estrategia de negocios, que determina la construcción del modelo operativo, la estructura de la organización y la arquitectura de información.

2.2.2.1- Análisis de Entorno

El análisis del entorno identifica las condiciones del ambiente, que influyen sobre la empresa. El objetivo es evaluar fuerzas, debilidades, oportunidades y riesgos del sector.

Las fuerzas y debilidades involucran la investigación del mercado doméstico, la carga financiera, productos, mercados, administración, estructura, cultura y recursos financieros de la empresa. En este análisis se debe buscar una comparación ("benchmarking") con el estado de las empresas relacionadas. El análisis de oportunidades y los riesgos, están relacionados con el estudio de consumidores, competidores y políticas del ambiente externo, como alianzas estratégicas, poder adquisitivo, costos de abastecimiento, etcétera. Estos aspectos pueden estar presentes ahora y/o pueden presentarse también en el futuro, influyendo sobre la estrategia de negocios, la operación administrativa y los sistemas de la organización.

2.2.2.2- Estrategia de Negocios

La estrategia de negocios se divide en: estrategia organizacional, competencias fundamentales y estrategia competitiva. La estrategia de negocios es un proceso que tiene que ver con la identificación de la visión, misión, objetivos, metas, estrategias y factores críticos de éxito (FCEs). Su definición se establece a través de una interrelación, una referencia cruzada simétrica y bidireccional, entre los elementos que unos con otros componen las estrategias, las entidades externas y el entorno de la organización. Las competencias fundamentales están relacionadas con las fortalezas de una organización. La estrategia competitiva establece que el éxito de

una empresa radica en satisfacer las necesidades de un cliente, ofreciéndole un valor agregado. Involucra cualidades de servicio, precio, confianza, imagen, etcétera, que hacen que un producto sea identificado como único y diferente. En este paso la influencia de la TI es determinante. Puede dar un valor agregado a servicios, productos y competencia, cambiando la manera como los negocios son llevados a cabo. Algunas de las estrategias competitivas más comunes se basan en el establecimiento de una diferenciación, bajos costos, enfoque específico e innovación

2.2.2.3.- Modelo Operativo

El modelo operativo se enfoca en el análisis y la reestructuración del funcionamiento de la empresa. Es un paso fundamental como precursor en la identificación de requerimientos de TI. Su naturaleza de diseño varía, de reestructuraciones radicales o reingeniería de procesos, a escenarios con un crecimiento gradual llamado modelado incremental. Es una perspectiva menos drástica, que intenta mejorar lo que ya existe.

Su diseño es una representación funcional de las estrategias de la organización. Se basa en un mecanismo que describe y refina, hasta un nivel operativo, las estrategias de negocio, transformándolas en procesos de un modelo operativo que detallan el comportamiento de la organización.

Un grafo acíclico dirigido se utiliza para representar el proceso jerárquico de refinamiento de las estrategias de negocios. Los sub grafos, enraizados en los hijos del nodo raíz, denotan todas las sub estrategias operativas de negocio o caminos posibles que se pueden tomar para refinar las estrategias globales.

Nótese que un proceso es un conjunto parcialmente ordenado de pasos, que intentan alcanzar los objetivos dados, en concordancia con el planteamiento de la estrategia de negocios. El proceso de refinamiento es diferente de otros estudios, en los que se construye una estructura jerárquica compuesta sólo de objetivos y sub objetivos.

Uno de los formalismos más prometedores, que constituye un marco metodológico para describir en detalle y sin ambigüedad el comportamiento de un modelo operativo, está basado en redes de Petri y sus extensiones, en redes de Petri de alto nivel. Estas últimas están relacionadas con "color", "tiempo" y "jerarquía", entre otras. Sus fundamentos matemáticos sólidos la convierten en una herramienta sofisticada de especificación, análisis y diseño organizacional.

Una red de Petri consiste en un grafo dirigido, cuyos nodos son lugares y transiciones, y cuyos arcos representan flujos de control que establecen la secuencia lógica de aplicación de los nodos. Los lugares están representados por círculos y las transiciones, por cuadrados. El diagrama 2.1 representa el proceso de solicitud de un pedido.

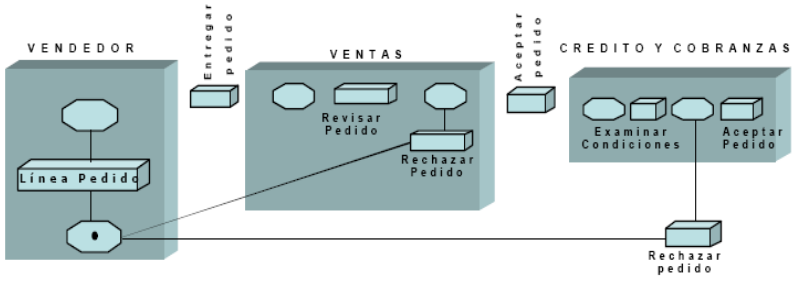


Diagrama 2.1: Ejemplo de un Modelo Operativo

2.2.2.4.- Estructura de la Organización

La estructura de la organización determina los aspectos de la administración de recursos humanos (papel, perfiles, responsabilidades, etcétera) y la conformación de la estructura de puestos del personal. Su construcción es una consecuencia lógica de las estrategias de negocios y el modelo operativo de la organización. Técnicas de "clúster", que integren la dinámica de las estrategias de negocios, pueden ser utilizadas para establecer la interrelación entre los puestos organizacionales.

2.2.2.5.- Arquitectura de Información

La arquitectura de información es una representación de los requerimientos globales de información, que la organización requiere para ejecutar sus actividades día a día. Se desarrolla para determinar las interrelaciones lógicas de los datos que soportan la operación de una empresa. Está relacionada con las necesidades de información que soportan la operación de la organización. Es independiente de cualquier consideración física y es cercana a las percepciones humanas del dominio del problema.

2.2.3.- Modelo de TI

La tercera fase está relacionada con la creación de un modelo de TI, que defina los lineamientos, controle las interfaces y establezca la integración de los componentes tecnológicos. El propósito es identificar soluciones de TI para establecer una ventaja estratégica y competitiva, así como el soporte operacional correspondiente.

2.2.3.1.- Estrategia de TI

La estrategia de TI está relacionada con los esfuerzos de diseño de implantación de TI, para soportar las estrategias de negocio de una empresa. Determina los lineamientos informáticos que deberán cumplir software, hardware y comunicaciones, para formar parte de la arquitectura informática.

Explícitamente, es un conjunto de lineamientos estratégicos, establecidos para relacionar el desarrollo del modelo de TI con la dirección estratégica del negocio y el comportamiento de la organización, permitiendo a la empresa alcanzar una ventaja estratégica y competitiva.

Tiene que ver con la identificación, formulación, entendimiento y refinamientos del propósito, política y dirección tecnológica de la organización. La importancia del proceso de definición de la estrategia de TI, está en transformar la estrategia de negocios en lineamientos de TI. Algunos autores conceptúan la relación entre la planeación estratégica de negocios y la planeación de SI, proponiendo una metodología para transformar la estrategia organizacional en una estrategia de SI.

Por ejemplo, suponga que las estrategias de una empresa pretenden desarrollar un alto grado de descentralización en la autoridad de sus ejecutivos, debido a la dispersión geográfica de sus áreas funcionales. La estrategia de TI podría incorporar tecnología que soporte: diseño de bases de datos distribuidas, sistemas de información soportados por modelos de datos sofisticados, sistemas de información ejecutiva orientados a diferentes niveles de mando, entre otros.

Un aspecto importante de la correspondencia entre las estrategias, es que la TI es desarrollada como parte integral de la organización. El proceso de transformación requiere la interacción de ejecutivos de negocios con expertos en TI. Esto permite a los ejecutivos revisar si los planteamientos estratégicos de TI son afines con la estrategia de negocios, y determinar su capacidad en la producción de los resultados esperados

2.2.3.2.- Arquitectura de Sistemas de Información

La arquitectura de sistemas de información determina el portafolio de aplicaciones necesario para sostener las estrategias, operación y estructura de la organización. Es fundamental en el proceso de planeación, ya que:

- Determina la visión global de los recursos de información, definiendo su alcance y asegurando su integración con los otros sistemas de información.
- Establece el orden de desarrollo de los sistemas, en base a su precedencia natural.
- Clarifica la relación que existe entre las aplicaciones y las necesidades de información de las áreas funcionales.

Su construcción se basa en el establecimiento de las relaciones que existen entre las clases de objetos de la arquitectura de información y los procesos del modelo operativo.

Las técnicas de "clúster", que integren la dinámica propuesta por las estrategias de negocios, pueden ser utilizadas para establecer la interrelación entre las aplicaciones, como se muestra en el ejemplo de la diagrama 2.2

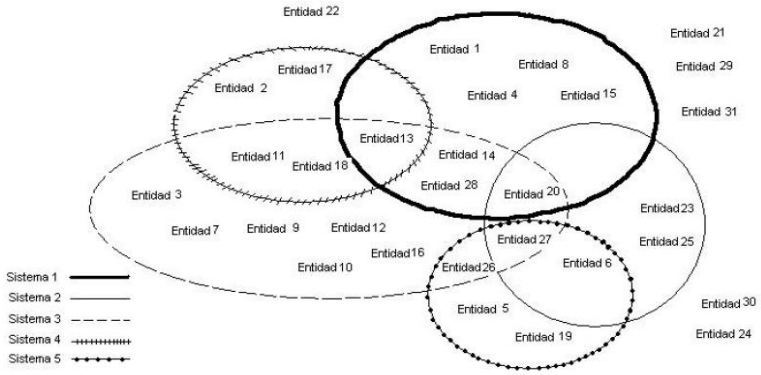


Diagrama 2.2: Ejemplo de Interrelación de los Sistemas de Información**.**

La arquitectura de SI se compone de sistemas de información (ver diagrama 2.3) desarrollados para soportar las actividades funcionales tradicionales de operación, monitoreo/control, planeación y toma de decisiones. Estas aplicaciones se utilizan para reducir costos de operación, mejorar la calidad y la eficiencia del trabajo, y darle a la organización la oportunidad de competir. En general no tienen ninguna relación con proveedores, consumidores y con el mundo externo.

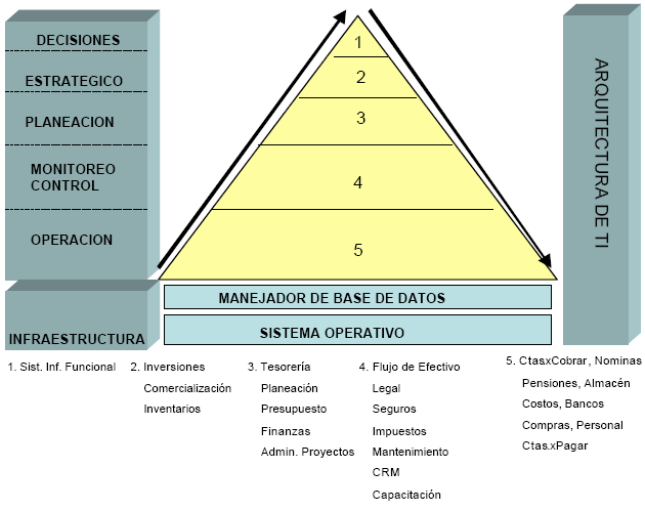


Diagrama 2.3: Arquitectura de Información

Asimismo, cuenta con SI estratégicos, desarrollados con la intención de producir iniciativas de negocio, como crear nuevos productos y penetrar en nuevos mercados, llegando directamente hasta el usuario final con un valor agregado. Estas aplicaciones surgen a partir de la percepción de los altos ejecutivos, como armas para soportar y generar una diferencia competitiva.

La planeación exige buscar y seleccionar, entre diversas alternativas, las aplicaciones que mejor se adapten a las necesidades de la empresa. Es por eso que una vez establecida la arquitectura de sistemas, es necesario evaluar las características funcionales y los costos de las aplicaciones existentes en el mercado. Esto se lleva a cabo considerando los lineamientos establecidos en la estrategia de TI que deben cumplir los proveedores. También es importante establecer tiempos y costos de desarrollo, en caso de que no exista un proveedor que cumpla con las características requeridas; los costos sean elevados, o que la aplicación sea innovadora.

2.2.3.4.- Arquitectura Tecnológica

Una vez definida la arquitectura de sistemas, el siguiente paso involucra la especificación de los elementos clave y las características esenciales de la arquitectura tecnológica (diagrama 2.4), que incluye la especificación de computadoras, impresoras, redes de computadoras, puertos, etcétera.

En este módulo se establecen los componentes tecnológicos; el lugar donde los sistemas y procesos van a correr; las características de almacenamiento de datos; la ubicación de los usuarios, y la manera cómo van a estar conectados.

Esta tarea se lleva a cabo considerando como antecedente la arquitectura de SI y el modelado de la organización.

Ambos permiten establecer el detalle de las necesidades de hardware y redes de comunicaciones.

Al igual que en el módulo anterior, es necesario buscar y seleccionar la infraestructura tecnológica que mejor se adapte a las necesidades de la empresa y establecer sus costos.

Esto se lleva a cabo, considerando los lineamientos establecidos en la estrategia de TI que deben cumplir los proveedores.

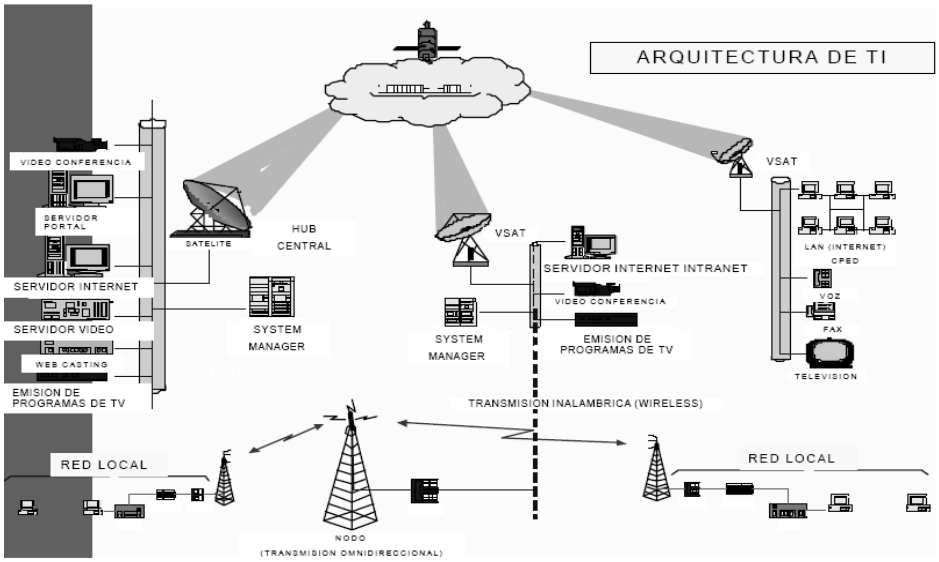


Diagrama 2.4: Esquema Genera de la Arquitectura de TI

2.2.3.5.- Modelo Operativo Informático

El modelo operativo informático se enfoca al análisis y la reestructuración del funcionamiento del área de sistemas. Su principal objetivo es identificar oportunidades para mejorar los procesos relacionados con el desarrollo, incorporación y sustento de TI.

Su construcción, al igual que el modelo operativo de la organización, está soportada por una reingeniería de procesos o un modelado incremental. Se basa en un refinamiento de las estrategias de negocio y las estrategias de TI hasta un nivel operativo, y en una transformación de las mismas en procesos funcionales que modelan el comportamiento de la función informática.

Diagrama 2.5: Modelo de la estructura de la Organización Informática

La estructura de la organización informática (diagrama 2.5) determina los aspectos de la administración de los recursos humanos en TI (organización, perfiles, entrenamiento, etcétera) y la conformación de la estructura de puestos del personal informático. Su finalidad es sustentar la función de TI, en la medida que la organización incorpora hardware, software y comunicaciones, así como en la conformación de la estructura de la organización, pueden ser utilizadas técnicas de "clúster" para establecer la interrelación entre los puestos informáticos.

El personal del área informática es variado: involucra expertos en análisis, así como el diseño de sistemas y comunicaciones, entre otros. Las funciones que realizan comprenden el establecimiento de estándares, la comunicación con los usuarios, el diseño de bases de datos, el desarrollo de diccionarios de datos, el desarrollo del PETI, la capacitación y el desarrollo de documentación, entre otros.

2.2.4.- Modelo de Planeación

2.2.4.1.- Prioridades de Implantación

La cuarta y última fase se vincula con la creación de un modelo de planeación, relacionado con la identificación de proyectos que muestren cómo los recursos van a ser incorporados en la organización. Se concentra en el establecimiento de sus prioridades, la creación de un plan, un estudio del retorno de la inversión y un análisis del riesgo.

El establecimiento de las prioridades es un método que permite colocar, en el orden debido de implantación, los procesos automatizables del modelo operativo y los traducidos en sistemas de información, esto en términos del potencial de ganancia y la probabilidad de éxito.

Está soportado por la amalgamación gráfica o por la matriz de Holmes. Que consiste en la calificación de factores. Una vez que se establece el peso de los factores, se procede a la evaluación de los factores dentro de las estrategias y finalmente, se calcula el peso de cada estrategia para determinar el orden de implantación.

Tabla 2.2: Matriz de Holmes

	F1	F2	F3	F4	F5	F6	F7	Suma	Impacto
F1	0.5	0	1	1	1	0	0	3.5	14%
F2	1	0.5	1	1	1	1	1	6.5	25%
F3	0	0	0.5	1	1	0	0	2.5	10%
F4	0	0	0	0.5	1	0	0	1.5	6%
F5	0	0	0	0	0.5	0	1	1.5	6%
F6	1	0	1	1	1	0.5	1	5.5	22%
F7	1	1	1	1	0	0	0.5	4.5	18%
							Total	25.5	

Luego de establecer el impacto de cada factor, se evalúa el peso de los mismos con respecto a las estrategias, dándonos como resultado el peso de cada proyecto para determinar el orden de implementación.

Tabla 2.3 Peso de Factores en las Estrategias.

	F1	F2	F3	F4	F5	F6	F7	Suma
E1	0.41	1.27	0.49	0.29	0.29	1.08	0.35	**4.20**
E2	0.69	0.51	0.29	0.18	0.06	0.43	0.71	**2.86**
E3	0.27	0.25	0.20	0.12	0.06	0.43	0.88	**2.22**
E4	0.34	0.51	0.29	0.43	0.29	0.88	0.29	**3.05**
E5	0.29	0.29	2	0.29	0.29	1.08	0.35	**4.61**

2.2.4.2.- Plan de Implantación

El plan de implantación determina la secuencia de proyectos que contribuyen a la creación de la PETI, dando una estimación del tiempo de duración. Cada proyecto especifica los pasos intermedios y la sincronización de todas las actividades para alcanzar los objetivos. La secuencia de implantación está determinada por el orden establecido en el módulo anterior. Los sistemas de información prioritarios serán

aquellos que brinden mayor beneficio a la empresa y que, por orden natural, deban ser implantados primero.

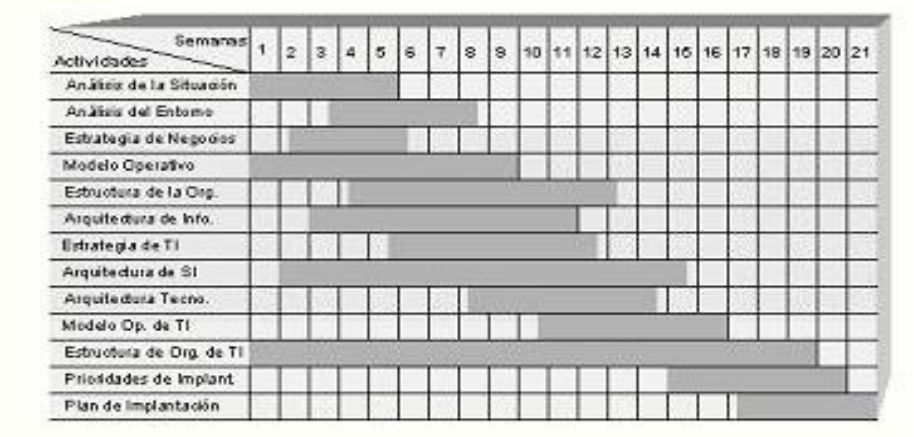


Diagrama 2.6: Cronograma de la implantación del Plan.

Las técnicas de planeación son variadas. Un diagrama de PERT o un CPM (método de ruta crítica) puede ser utilizado para establecer la secuencia y estimar los tiempos de duración de los proyectos. El calendario puede ser representado a través de una gráfica de Gantt (Diagrama 2.6). Su tarea principal es formalizar las fechas de inicio y fin de un proyecto, así como establecer puntos de control para la supervisión del plan de implantación.

2.2.4.3.- Retorno de la Inversión

El retorno de la inversión es un estudio de viabilidad de la PETI, basado en un análisis costo/beneficio. Un costo es un desembolso de recursos para la organización, asociado con la implementación de tecnología de información, un modelo operativo o la incorporación de recursos humanos. Generalmente es representado en términos monetarios. Los costos de un proyecto de desarrollo de

sistemas pueden estimarse con bastante precisión, teniendo una especificación de los tiempos y los recursos humanos necesarios.

En particular, los costos de hardware y software son fáciles de obtener a través de entrevistas con los proveedores.

Un beneficio es una mejora o contribución para la organización. Obviamente está asociado con la implementación de tecnología de información, el modelo operativo o la incorporación de recursos humanos. Tradicionalmente son clasificados como tangibles o intangibles. En ambos casos, un valor monetario está asociado con ellos. Desgraciadamente no siempre es fácil convertir los beneficios en dinero.

2.2.4.4.- Administración del Riesgo

La administración del riesgo se encarga de reconocer la existencia de amenazas, determinando sus orígenes y consecuencias. Además trata de aplicar factores de modificación para contrarrestar situaciones adversas. Las estrategias para administrar el riesgo dependen, principalmente, de la naturaleza del riesgo y las variables asociadas que influyen en el rango de opciones de una empresa.

Los cuatro métodos principales para combatir el riesgo, son:

1. Reducción. Apoyada en acciones para la eliminación o disminución del riesgo;
2. Protección. Relacionada con elementos físicos para la eliminación o reducción del riesgo;
3. Transferencia. Orientada a la delegación de responsabilidades a terceros, y
4. Financiamiento. Sustentado en la adopción de métodos para el control de inversiones.

2.3.- CONCEPTOS BÁSICOS Y DEFINICIÓN DE SEGURIDAD INFORMÁTICA

La seguridad Informática actualmente ha tenido que evolucionar a pasos agigantados debido a las cambiantes condiciones y nuevas plataformas disponibles.

Desde un inicio con la posibilidad de interconectarse a través de Redes, primero locales y luego internacionales lo cual ha permitido a las empresas mejorar en todo ámbito su productividad (oferta); pero ha traído consigo nuevas amenazas para los Sistemas Informáticos e información confidencial.

Las políticas tomadas en cuenta dentro de la seguridad informática nacen o aparecen como una herramienta organizacional para concientizar al personal de las empresa u organización sobre la importancia de la información y el peligro al cual está expuesta; ante esto, el proponer o identificar una política de seguridad requiere un alto compromiso con la organización, poder determinar y establecer fallas y debilidades, constancia para renovar y actualizar dicha política en función del cambio constante y ambiente organizacional.

El propósito de establecer un plan de Seguridad Informática es proteger la información junto con los activos de la organización, tratando de conseguir confidencialidad, integridad, disponibilidad de los datos y responsabilidades que debe asumir cada uno de los empleados de la organización.

2.3.1.- Dato

Es el elemento primario de la información conformado por símbolos (letras, números, dibujos, señas, gestos) que reunidos pueden cobrar significación. Solo o

aislado el dato no posee relevancia, pero una vez procesado puede brindar soluciones, conclusiones, etc.

2.3.2.- Información

Es un conjunto de datos que están organizados, procesados y clasificados, los cuales constituyen una información útil y funcional; todo aquello que nos brinda conocimiento se lo considera información.

Cualquiera que no tenga un conocimiento suficiente necesita de información para tomar sus decisiones. En toda organización es necesaria la información, que surge como consecuencia de las actividades que se llevaran a cabo para alcanzar sus objetivos.

La información se reconoce como:

- Crítica, indispensable para garantizar la continuidad operativa de la organización.
- Valiosa, es un activo corporativo que tiene valor en sí mismo.
- Sensitiva, debe ser conocida por las personas que necesitan los datos.

2.3.3.- Seguridad

Medidas de resguardos contra el acceso no autorizado a los datos, consiste en proteger una de las partes más importantes del negocio, la información; así como también proteger el espacio y estado físico de todos y cada uno de los equipos existentes en la organización**.** Conviene aclarar que no siendo posible la certeza

absoluta, el elemento de riesgo está siempre presente, independiente de las medidas que tomemos.

2.3.4.- Amenazas

Una amenaza es un fenómeno o proceso natural, causado por el ser humano que puede poner en peligro a un grupo de personas, sus cosas y su ambiente.

Es todo aquello que pone en riesgo de pérdida, alteración, daño, a la información y a los ordenadores de una organización así como también cualquier elemento que comprometa a los sistemas.

2.3.5.- Riesgos

El riesgo está presente casi siempre en todas las actividades que el hombre realiza, es por esto que antes de implementar cualquier mecanismo de seguridad (software, hardware, política, etc.) en el área informática, es necesario conocer la prioridad de la aplicación y qué tipo de medida se puede aplicar.

2.3.6.- Salvaguardas

Una salvaguarda o contramedida es cualquier cosa que ayuda a detener las amenazas sobre nuestros activos, las salvaguardas deben ser definidas para cada uno de los riesgos analizados para poder contrarrestarlos

2.3.7.- Seguridad Informática

Consiste en garantizar que los recursos informáticos (Equipos, Software) estén disponibles a cualquier momento y sean utilizados de manera correcta, así como también asegurar la integridad y privacidad de la información.

Se puede definir entonces a la seguridad informática como la disciplina que se relaciona a diversas técnicas, establecidas para prevenir, proteger y resguardar todo aquello susceptible de robo, pérdida o daño, ya sea de manera personal, grupal o empresarial.

"El objetivo de la seguridad informática será mantener la Integridad, Disponibilidad, Privacidad (sus aspectos fundamentales), Control y Autenticidad de la información manejada por computadora."[1]

Todo lo que la seguridad informática dispone a resguardar por todos aquellos riesgos presentes y que son motivo de análisis, se separan en dos escenarios, Seguridad Lógica y Seguridad Física.

2.3.8.- Plan De Seguridad Informática

Constituye el documento básico que establece los principios organizativos y funcionales de la actividad de Seguridad Informática en una entidad y recoge claramente las políticas de seguridad y las responsabilidades de cada uno de los participantes en el proceso informático, así como las medidas y procedimientos que permitan prevenir, detectar y responder a las amenazas que gravitan sobre el mismo.

---

[1] ALDEGANI, Gustavo. Miguel. Seguridad Informática. MP Ediciones. Argentina. 1997. Página 22.

Como una política de seguridad debe orientar las decisiones que se toman en relación con la seguridad, se requiere la disposición de todos los miembros de la empresa para lograr una visión conjunta de lo que se considera importante.

Las políticas de seguridad informática, deben ofrecer explicaciones comprensibles sobre por qué deben tomarse ciertas decisiones y explicar la importancia de los recursos. Igualmente, deberán establecer las expectativas de la organización en relación con la seguridad y especificar la autoridad responsable de aplicar los correctivos o sanciones.

Por último, y no menos importante, el que las políticas de seguridad, deben seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes, como son: el aumento de personal, cambios en la infraestructura computacional, alta rotación de personal, desarrollo de nuevos servicios, regionalización de la empresa, cambio o diversificación del área de negocios, etc.

2.3.9.- Definición De Políticas De Seguridad

Una política de seguridad es un conjunto de directrices, normas, procedimientos e instrucciones que guía las actuaciones de trabajo y define los criterios de seguridad para que sean adoptados a nivel local o institucional, con el objetivo de establecer, estandarizar y normalizar la seguridad tanto en el ámbito humano como en el tecnológico.

A partir de sus principios, es posible hacer de la seguridad de la información un esfuerzo común, en tanto que todos puedan contar con un arsenal informativo documentado y normalizado, dedicado a la estandarización del método de operación

de cada uno de los individuos involucrados en la gestión de la seguridad de la información.

La política se elabora considerando el entorno en que se está trabajando como la tecnología de la seguridad de la información, para que los criterios establecidos estén de acuerdo con las prácticas internas más recomendadas de la organización, con las prácticas de seguridad actualmente adoptadas, para buscar una conformidad mayor con criterios actualizados y reconocidos en todo el mundo

En la actualidad la ausencia de políticas de seguridad en las empresas, puede ocasionar efectos catastróficos en los negocios de éstas.

2.3.10.- Importancia del Plan de Seguridad Informática

Después de conocer las amenazas y puntos débiles del ambiente, adquiridos en el análisis de riesgos, o después de la definición formal de las intenciones y actitudes de la organización que están definidas en la política de seguridad de la información, debemos tomar algunas medidas para la implementación de las acciones de seguridad recomendadas o establecidas.

Recuerde que las amenazas son agentes capaces de explotar fallos de seguridad, que denominamos puntos débiles y, como consecuencia de ello, causan pérdidas o daños a los activos de una empresa y afectan sus negocios. No basta conocer las fragilidades del ambiente o tener una política de seguridad escrita.

Se debe instalar herramientas, divulgar reglas, concienciar a los usuarios sobre el valor de la información, configurar los ambientes etc. Debemos elegir e implementar cada medida de protección, para contribuir con la reducción de las vulnerabilidades; cada medida debe seleccionarse de tal forma que, al estar en

funcionamiento, logre los propósitos definidos. Gran parte de esa concientización está en manos de los responsables de seguridad de la información apoyados en todo momento por la Gerencia de forma explícita y activa, por ello es importante indicarles no sólo cuales son las principales amenazas en cada momento, sino qué deben hacer para evitarlas

2.4.- ANÁLISIS Y GESTIÓN DE RIESGOS

Análisis de riesgo es el proceso cuantitativo o cualitativo que permite evaluar los riesgos; determina cómo es, cuánto vale, cómo y cuan protegidos se encuentran los activos. En coordinación con los objetivos, estrategia y política de la organización, las actividades de gestión de riesgos permiten elaborar un plan de seguridad que, implantado y operado, satisfaga los objetivos propuestos con el nivel de riesgo que se acepta la Dirección

2.4.1.- Gestión o Administración

La gestión de riesgo en la seguridad informática ofrece a las organizaciones algunos métodos y herramientas sencillas, con el propósito de reconocer la importancia y la urgente necesidad de incorporar la seguridad informática en sus procesos operativos institucionales, para proteger y garantizar no solamente el cumplimiento de sus misiones institucionales, sino también la privacidad y los derechos de sus activistas, aliados y sobre todo de sus beneficiarios

La gestión de riesgo es un método para analizar, clasificar, reducir y controlar el riesgo, para posteriormente implementar mecanismos que permitan controlarlo.

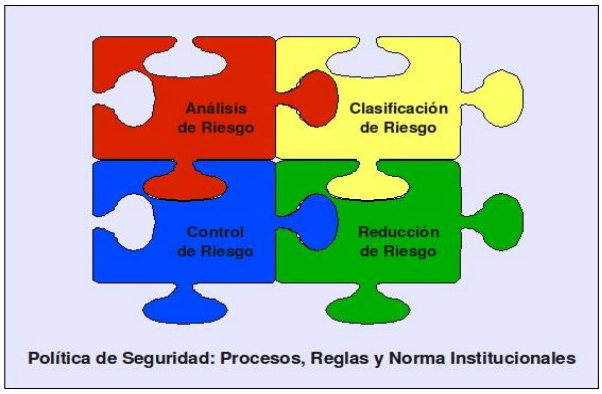


Diagrama 2.7 Política de Seguridad

2.4.1.1.- Análisis

El análisis de riesgo es un proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una organización o empresa.

Es la identificación de las amenazas que asechan a los distintos componentes pertenecientes o relacionados con un sistema de información para determinar la vulnerabilidad del sistema ante esas amenazas y para estimar el impacto o grado de perjuicio que una seguridad insuficiente puede afectar a la organización.

2.4.1.2.- Identificación y Clasificación

Permite determinar y establecer que riesgos son factibles de combatir o contrarrestar, esto no solo dependerá de la voluntad y posibilidad económica de una institución, sino también del entorno donde se ubica. Existirán riesgos que no podrán ser combatidos y tendrán que ser aceptados por la misma.

2.4.1.3.- Reducción

La reducción de riesgos se dará cuando se hayan establecido políticas, medidas o salvaguardas una vez analizados y clasificados los riesgos.

2.4.1.4.- Control

El control es dar seguimiento, verificar efectividad, funcionamiento y cumplimento a las medidas de protección establecidas

Medir el cumplimiento y la efectividad de las medidas de protección requiere que se levanten constantemente registros sobre la ejecución de las actividades, los eventos de ataques y sus respectivos resultados.

2.4.2.- Metodología para el Análisis de Riesgos

La metodología de análisis y gestión de riesgos de los sistemas de Información, MAGERIT, es un método formal para investigar los riesgos que soportan los Sistemas de Información, y para recomendar las medidas apropiadas que deberían adoptarse para controlar estos riesgos.

La generalización del uso de las tecnologías de la información y de las comunicaciones es potencialmente beneficiosa para los ciudadanos, las empresas, pero también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza en su utilización.

No es posible una aplicación racional de medidas de seguridad sin antes analizar los riesgos para, así implantar las medidas proporcionadas a estos riesgos,

al estado de la tecnología y a los costes (tanto de la ausencia de seguridad como de las salvaguardas).

El análisis de los riesgos generados por el uso de sistemas informáticos determina las políticas de seguridad en los sistemas de Información mediante:

- Planificación de la seguridad
- Implantación de salvaguardias (Implicación de todos los recursos humanos e informáticos en los sistemas de seguridad)
- Seguimiento de los sistemas de seguridad (Reacción a los eventos, registros de incidencias y recuperación de estados de seguridad)

2.4.2.1.- Clasificación de Activos e Información

Una vez que se hayan detectado procesos críticos y sistemas informáticos dentro de la organización es necesario analizar y clasificar activos (Software, hardware, Servicios) e información.

La tipificación de los activos es tanto una información documental de interés como un criterio de identificación de amenazas potenciales y salvaguardas apropiadas a la naturaleza del activo.

2.4.2.2.- Jerarquización de las Aplicaciones

Es necesario definir anticipadamente cuales son las aplicaciones primordiales para la organización.

El plan debe incluir una lista de los sistemas, aplicaciones y prioridades, igualmente debe identificar aquellos elementos o procedimientos informáticos como

el hardware, software básico, de telecomunicaciones y el software de aplicación, que puedan ser críticos ante cualquier eventualidad o desastre y jerarquizarlos por orden de importancia dentro de la organización.

2.4.2.3.- Pilar, Ris2k, Chinchón

Los activos están expuestos a amenazas que, cuando se materializan, degradan el activo, produciendo un impacto. Si estimamos la frecuencia con que se materializan las amenazas, podemos deducir el riesgo al que está expuesto el sistema. Degradación y frecuencia califican la vulnerabilidad del sistema.

El gestor del sistema de información dispone de salvaguardas, que o bien reducen la frecuencia de ocurrencia, o bien reducen o limitan el impacto. Dependiendo del grado de implantación de estas salvaguardas, el sistema pasa a una nueva estimación de riesgo que se denomina riesgo residual.

Para esto se dispone de algunas herramientas entre las cuales se destacan Pilar, Ris2k y Chinchón, siendo el primero el mas actualizado y con el que se trabajara en el plan.

2.5.- METODOLOGÍA DEL PLAN SE SEGURIDAD INFORMÁTICA (NORMA ISO 27002)

Esta Norma ISO pretende poder ser implementada en todo tipo de empresa, y en cualquier tipo de negocio; básicamente especifica los requerimientos para establecer, implementar, operar, monitorear, revisar y mantener documentado la seguridad de la información en la administración de sistema.

Algunos de los puntos sobre los cuales la Norma ISO trabaja son:

- Las organizaciones la usen como un modo de asegurar que los costos que ameritan los riesgos en la seguridad se encuentren monitoreados de manera efectiva
- Asegurar que los objetivos de seguridad dentro de la empresa son conocidos por todo el personal
- Definición de nuevos procesos en cuanto a seguridad de información se refiere
- Clarificar dentro de una organización cual es su grado de madurez en cuanto a seguridad de Información.
- Obtener información importante de políticas, estándares, procedimientos dentro de la Seguridad de la Información que se encuentran presentes al momento de trabajar con terceras partes cuando de proveedores de software o hardware se refiere.

2.5.1.- Política de seguridad.

Son una forma de comunicación con el personal, ya que las mismas constituyen un canal formal de actuación, en relación con los recursos y servicios informáticos de la organización. Estas a su vez establecen las reglas y procedimientos que regulan la forma en que una organización previene, protege y maneja los riesgos de diferentes daños, sin importar el origen de estos.

Una política de seguridad bien planteada, diseñada, y desarrollada cubre la gran mayoría de los aspectos que hacen falta para un verdadero SGSI.

2.5.2.- Organización de la información de seguridad.

Se trabaja sobre el hecho de definir el personal responsable que se encargara del mantenimiento, revisión y de evaluación periódicamente, si las políticas antes elaboradas son correctas, si fallan, si están completas, si pueden mejorarse, etc.

2.5.3.- Administración de recursos

Es un requisito sine qua non de toda empresa, llevar un inventario completo de que es lo que se posee, y que nivel de actualización se tiene, este grupo aclara que todo recurso se debe encontrar inventariado con el máximo nivel de detalle y se debe documentar el uso adecuado de los mismos.

2.5.4.- Seguridad de los recursos humanos.

La mayoría de empresas no tienen claro que el área de RRHH debe trabajar de la mano con el Área de Sistemas. Se debe partir por la redacción de la documentación necesaria para la contratación de personal y la revocación de sus contratos (por solicitud, cambio o despido). En la misma deberá quedar bien claro las acciones a seguir para los diferentes perfiles de la organización, basados en la responsabilidad de manejo de información que tenga ese puesto.

2.5.5.- Seguridad física y del entorno

Este grupo trabaja con el objetivo de mejorar todo lo que se refiere a seguridades lógicas que vienen a ser todas las aplicaciones instaladas dentro de una organización, seguridades de hardware o equipos, mantenimiento de los mismos, seguridades en cuanto a transporte que se refiere a transmisión de datos, seguridad en redes que abarca el hecho de segmentar, troncalizar, etc., la red de una organización; y por ultimo seguridad física en cuanto a control de accesos, control de corriente eléctrica e infraestructura.

2.5.6.- Administración de las comunicaciones y operaciones

Tiene como objetivo asegurar la correcta y segura operación de la información; hace especial hincapié en documentar todos los procedimientos, manteniendo los mismos disponibles a todos los usuarios que los necesiten; así como documentar de manera correcta los servicios o tareas que se estén prestando por parte de terceros (acuerdos, obligaciones, responsabilidades, confidencialidad, operación, mantenimiento, etc.).

Planificar todo tipo de cambios en cuanto a sistemas se refiere para así poder reducir el riesgo de fallos al momento de arrancar o poner en producción nuevos requerimientos, trabajar en ambientes los cuales sean muy semejantes a la realidad y poder trabajar con el sistema e información que la empresa maneje y ver así el desenvolvimiento de las actualizaciones.

Administrar y controlar todo lo que se refiere a la red empresarial, es decir, implementar todas las medidas posibles para evitar amenazas, manteniendo la

seguridad de los sistemas y aplicaciones a través del conocimiento de la información que circula por ella

Prevenir la difusión, modificación, borrado o destrucción de cualquier medio magnético en el cual haya sido previamente almacenado información, mediante medidas que aseguren su almacenamiento seguro y uso incorrecto de los mismos.

Mantenimiento de logs en todos los aplicativos que organización posea para así poder controlar accesos y evitar que cualquier intruso borre sus huellas.

No permitir el intercambio de información sea o no en línea, recalquemos que la información es el bien más preciado de una organización; por esto el intercambio de información debe ser llevado a cabo mediante reglas y usuarios establecidos.

2.5.7.- Control de accesos

Este grupo esta direccionado a la actividad posterior a la autenticación dentro de un sistema; debe regular que el usuario autenticado, acceda únicamente a los recursos sobre los cuales tenga derecho y a ningún otro; esto a través de una Política de Control de accesos documentada, periódicamente revisada y basada en los niveles de seguridad que determine el nivel de riesgo de cada activo.

2.5.8.- Adquisición de sistemas de información, desarrollo y mantenimiento

Plantea la necesidad de realizar un análisis de los requerimientos que deben exigirse a los sistemas de información, desde el punto de vista de la seguridad para cumplir con las necesidades del negocio de cada empresa en particular, para poder garantizar que la seguridad sea una parte integral de los sistemas.

Así como también incluir dentro de los procesos, las etapas en cuanto a desarrollo se refiere (Análisis, Diseño, Implementación y Pruebas), documentar lo necesario y poder tener revisiones periódicas de las tareas a realizarse y poder cumplir con todo lo pedido o pactado con terceros.

2.5.9.- Administración de los incidentes de seguridad

Define el desarrollo de una metodología eficiente para la generación, monitorización y seguimiento de reportes, los cuales deben reflejar, tanto eventos de seguridad como debilidades de los sistemas, la mejor opción es implementar herramientas de detección de vulnerabilidades.

Se debe establecer también un procedimiento que describa claramente: pasos, acciones, responsabilidades, funciones y medidas concretas. Para lo cual se necesitara exista la preparación adecuada del personal, por lo tanto es necesario difundirlo, practicarlo y simularlo.

2.5.10.- Administración de la continuidad de negocio

Tiene como objetivo contemplar todas las medidas necesarias para que los sistemas no sufran interrupciones sobre la actividad que realiza la empresa.

Lo primero que considera este grupo es que la seguridad de la información se encuentre incluida en la administración de la continuidad de negocio.

2.5.11.- Marco Legal y buenas prácticas (legales, de estándares, técnicas y auditorías)

Se dice que este último grupo de controles es el más débil de la norma debido a que está limitado a las leyes de cada empresa o cada país.

Lo primero a considerar es la identificación de la legislación aplicable a la empresa, definiendo explícitamente y documentando todo lo que guarde relación con estos aspectos. Otro componente es lo relacionado con los derechos de propiedad

Intelectual, debiendo generar procedimientos que aseguren el cumplimiento de las regulaciones. Así como el hecho de obtener software legal e implementarlo con las respectivas licencias.

Este grupo trata además de las “Buenas prácticas”, ya que de que sirve implantar una normal basada en políticas, controles, procedimientos, etc., si luego el personal involucrado no da cumplimiento a las medidas y en definitiva, la implementación falla.

Por esto otro punto importante en esta norma es el hecho de realizar auditorías y tener herramientas de auditoría las cuales permitan dictar si la norma y procedimientos encadenados se estén cumpliendo a cabalidad o si la misma tiene debilidades.

2.6.- NORMA DE CONTROL GUBERNAMENTAL DE SEGURIDAD INFORMÁTICA

El complejo FAME S.A., es una organización la cual se podría decir es de carácter público; por ende es recomendable que tome en cuenta las normas estipuladas o establecidas por la Contraloría General del Estado de Control Interno para el Sector Público; orientadas a promover una adecuada administración de los recursos y a determinar el correcto funcionamiento administrativo de las entidades y organismos del sector público ecuatoriano, con el objeto de buscar la efectividad, eficiencia y economía en la gestión institucional.

Para el estudio, dentro de las normas de Control Interno para el Sector Público existe una que está totalmente relacionada:

- 400-00 ÁREA: Normas de control interno para el área de sistemas de información computarizados.

Dicha norma se enfoca en lo que es la planificación estratégica informática y la seguridad informática, brindando guías que permiten mejorar procedimientos existentes en la organización.

CAPÍTULO III

EVALUACIÓN SITUACIÓN ACTUAL DE LA ORGANIZACIÓN

3.1.- DESCRIPCIÓN DE LA ORGANIZACIÓN

3.1.1.- Identificación de la organización

FABRIL FAME S.A. es una empresa nacional que diseña, fabrica y comercializa vestuario, calzado y equipos de camping. Dispone de la marcas: FAME S.A., para elaborar ropa de trabajo, uniformes institucionales, uniformes escolares, ropa deportiva y calzado militar; Pietro Peruzzi y Jean Cartier, para la confección de la línea de ropa masculina y femenina; y Cover Camp para la producción de equipos de camping y calzado de trabajo.

La empresa del FABRIL FAME S.A. desarrolla sus actividades en cumplimiento con el ordenamiento jurídico establecido en la Ley de Compañías, Ley de Contratación Pública, Ley y Reglamento del Régimen Tributario, Reglamento General de Riesgos de Trabajo, Reglamento de Seguridad y Salud. Además aplica las normas AATCC, ASTM e ISO, para el control de materia prima

3.1.2.- Misión

Producir y comercializar vestuario, calzado y equipo de camping, de uso militar, institucional e industrial, con calidad y precios competitivos, para satisfacer las necesidades de las Fuerzas Armadas y del mercado nacional

3.1.3.- Visión

Ser líderes en la confección de vestuario, calzado y equipo de camping, en el mercado militar, industrial e institucional, a nivel nacional, con proyección regional. Socialmente responsables y comprometidos con el desarrollo del país.

3.1.4.- Estructura Organizacional

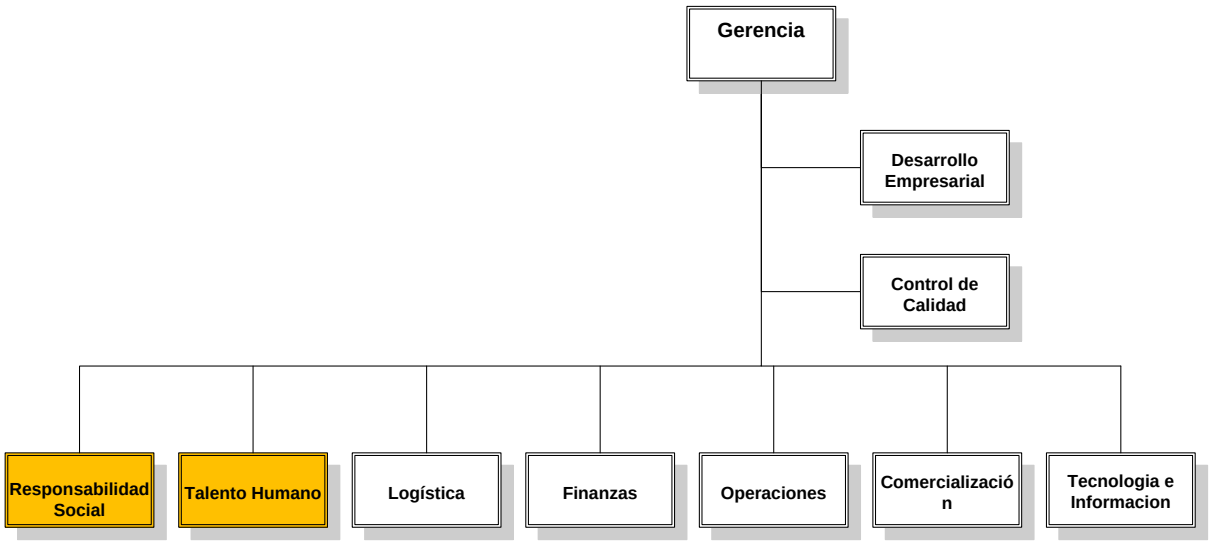


Diagrama 3.1: Organización de la Empresa Textil “FABRIL FAME SA”

3.2.- INFORME DE EVALUACIÓN DE FAME

3.2.1.- Informe Ejecutivo

El informe de evaluación o situación actual fue elaborado por el personal de la Empresa Textil Fabril Fame SA, la cual se encuentra ubicada en Sangolqui, Quito-Ecuador; este informe tiene como resultados la información provista por el personal ya nombrado y por las observaciones dadas al momento de realizar las visitas y entrevistas.

El informe fue elaborado de acuerdo a los controles expuestos en la norma ISO 27002:2005 mediante un cuestionario de investigación y las observaciones realizadas durante las visitas. Cada control fue evaluado dentro de la entidad para comprobar su cumplimiento.

3.2.2.- Introducción

Este informe de evaluación de la seguridad de la información de la empresa textil Fabril Fame S.A., ha sido preparado por estudiantes de la Escuela Politécnica del Ejército para elaboración del "Plan de Seguridad Informática de FAME", como parte del proyecto de grado previa la obtención del título de grado.

3.2.3.- Metodología

Para la elaboración de este informe se tomo como referencia la norma internacional ISO 27002:2005.

Esta norma tiene antecesores y tiene predecesores; los cuales en general dictan recomendaciones o buenas prácticas para implementar, mantener, monitorear controles que permitan una correcta gestión de seguridad de la información.

Este estándar está compuesto por once grupos o dominios, cada dominio se divide en objetivos de control, y estos a su vez contienen los controles para la seguridad de la información.

Cada control ha sido evaluado dentro de FAME, de los cuales se ha obtenido información proporcionada por el personal del Departamento de Tecnología e Información y observaciones que se presentaron en el proceso. Así se ha

determinado su cumplimiento total, parcial o nulo; en estos dos últimos se enfocara el informe que a continuación se presenta.

3.2.4.- Resultados de la Evaluación a la Empresa

3.2.4.1.- Dominio: Política de seguridad

Objetivo de control: Política de seguridad de la información

Control: Documento de política de seguridad de la información

Observación No 1

Título: Falta de una política de seguridad interna de la institución.

Norma: La Dirección debería aprobar y publicar un documento de la política de seguridad de la información y comunicar la política a todos los empleados y las partes externas relevantes.

Condición: Actualmente la empresa no dispone de un documento de políticas de seguridad de información

Evidencia: Cuestionario de investigación de la Seguridad de la información de FAME.

Riesgo: Carencia de conocimiento por parte del personal en el tema de seguridad de la información poniendo en riesgo la misma y dificultando su implantación y ejecución.

Causa: No existe una política para que sea publicada y aplicada con el fin de que el personal pueda cumplirla, tanto la dirección como el personal han puesto de lado y no han tomado en cuenta la posibilidad de generar el documento necesario.

Recomendaciones: La dirección de FAME debería elaborar una política de seguridad con sus objetivos y alcances generales explicando los requisitos de cumplimiento en materia de seguridad. Además el nivel gerencial debe ser responsable, apoyar y difundir los objetivos y principios de la seguridad de la información.

Control: Revisión de la política de seguridad de la información

Observación No 2

Título: Falta de revisión y mantenimiento de la política de seguridad de la información.

Norma: La política de seguridad de la información se debería revisar a intervalos planificados (o en caso que se produzcan cambios significativos) para garantizar que es adecuada, eficaz y suficiente.

Condición: Debido a la observación número uno, es obvio que esta norma no se podrá cumplir ya que no existe una política a la cual se le pueda dar seguimiento de cumplimiento y posibles modificaciones ante cualquier debilidad de la misma.

Evidencia: Cuestionario de investigación de la Seguridad de la información de FAME.

Riesgo: La empresa no cuenta con una política de seguridad de la información que pueda ser revisada, mantenida y probada de acuerdo a sus necesidades, provocando que el personal pueda ejecutar acciones que vayan contra la seguridad de la información.

Causa: Como la política documento de políticas no existe en la empresa, entonces no hay acción que tomar sobre la misma.

Recomendaciones: La política de seguridad de la información se debería revisar y mantener a intervalos planificados por un responsable; mediante un proceso definido para garantizar la eficacia de la política, para así poder tener claro el costo e impacto de cualquier riesgo que se pueda presentar o ya está presente.

3.2.4.2.- Dominio: Aspectos organizativos de la seguridad de la información

Objetivo de control: Organización interna

Control: Compromiso de la dirección con la seguridad de la información

Observación No 3

Título: Falta de compromiso de la dirección con respecto a la seguridad de la información

Norma: Los miembros de la Dirección deberían respaldar activamente las iniciativas de seguridad demostrando su claro apoyo y compromiso, asignando y aprobando explícitamente las responsabilidades en seguridad de la información dentro de la institución.

Condición: Existen reuniones trimestrales en las cuales se presentan informes, se definen presupuestos, se evalúa riesgos y amenazas, se aprueban nuevas ideas para controlar vulnerabilidades pero no existe el compromiso de la dirección con respecto a las políticas de seguridad, al parecer es un tema de desconocimiento, por lo tanto se puede decir que la seguridad de la información es hecha a mano sin planificación, sin mantenimiento, sin monitoreo.

Evidencia: Cuestionario de investigación de la seguridad de la información de FAME.

Riesgo: Por más que se realicen reuniones y se trate el tema de seguridad de información, sin política no hay control, por lo tanto cero planificación; esto recae en el hecho de no saber que amenazas existen o que acciones tomar antes cualquier suceso, pueden ser considerados algunos riesgos pero no todos solo por el hecho de no conocer la importancia de tener una política de seguridad de la información definida correctamente.

Causa: El desconocimiento en cuanto a Seguridad de Información es el causante de no cumplir con esta norma.

Recomendaciones: Es necesario que La Dirección tome acción sobre la Política de Seguridad de Información, ya que si bien es cierto existe apoyo en cuanto a presupuesto, nuevas ideas, reuniones periódicas, etc. Pero de nada sirve si no se sabe con certeza cuales son los objetivos de cada punto.

Control: Coordinación de la seguridad de la información

Observación No 4

Título: Falta de coordinación de seguridad de la información.

Norma: Las actividades para la seguridad de la información deberían ser coordinadas por representantes que posean de cierta relevancia en su puesto y funciones y de los distintos sectores que forman la institución.

Condición: Actualmente, si se tramita a nivel de directorio o gerencia, pero no se da la importancia de designar a una persona que conozca de Seguridad de Información, sino que se designa a alguien en caso de que algo se presente.

Evidencia: Cuestionario de investigación de la Seguridad de la información de FAME.

Riesgo: Las actividades que se realicen en cuanto a Seguridad de la información, quedan en el aire a espera de que alguien sea asignado; las mismas pueden no ejecutarse de manera correcta y al mismo tiempo quedan estancadas donde empezaron ya que no son difundidas al personal.

Causa: Falta de organización por parte de las autoridades en el campo de la seguridad de la información.

Recomendaciones: La Dirección y jefes de cada departamento deben coordinar las actividades con respecto a la seguridad de la información; deben acordar funciones, metodologías y responsabilidades y procesos específicos relativos a la seguridad de la información para toda la empresa.

Control: Asignación de responsabilidades relativas a la seguridad de la información

Observación No 5

Título: Falta de Documentación en cuanto a responsabilidades y niveles de autorización se refiere.

Norma: Se deberían definir claramente todas las responsabilidades para la protección de los recursos con sus procesos específicos de seguridad.

Condición: Las responsabilidades en cuanto a recursos se encuentran claras y el personal las conoce, pero no se encuentra documentado al igual que los niveles de autorización, los cuales son conocidos pero no están plasmados bajo un documento el cual especifique y obligue.

Evidencia: Cuestionario de investigación de la Seguridad de la información de FAME.

Riesgo: Los recursos tienen responsables a cargo pero solo mediante palabra, es decir que no tienen un claro conocimiento de sus responsabilidades.

Causa: Falta de una política de seguridad que suministre una orientación general acerca de la asignación de funciones de seguridad y responsabilidades dentro la organización.

Recomendaciones: Se debe definir el personal a cargo de cada recurso, mediante procesos escritos los cuales permitan al personal tener claro todo el cuadro de responsabilidades así como los niveles de autorización.

Control: Proceso de autorización de recursos para el procesado de la información

Observación No 6

Título: Falta de documentación en cuanto a gestión de autorizaciones para nuevos recursos de tratamiento de la información.

Norma: Se debería definir y establecer un proceso de gestión de autorizaciones para los nuevos recursos de tratamiento de la información.

Condición: No existe un proceso escrito de gestión de autorizaciones para cuando se requiere colocar una nueva instalación de procesamiento de información.

Evidencia: Cuestionario de investigación de la Seguridad de la información de FAME.

Riesgo: Si no hay un documento escrito, el proceso puede o no cumplirse a cabalidad, esto puede producir que las instalaciones presenten problemas.

Causa: Falta de un proceso claro, escrito y difundido que pueda controlar lo necesario a seguir.

Recomendaciones: Se debería establecer un proceso oral y escrito de autorización gerencial para nuevas instalaciones de procesamiento de información, el mismo debe ser difundido para que así las nuevas instalaciones sean aprobadas adecuadamente por la gerencia usuaria, autorizando su propósito y uso. La aprobación también debe obtenerse del gerente responsable del mantenimiento del ambiente de seguridad del sistema de información local, a fin de garantizar que se cumplen todas las políticas y requerimientos de seguridad pertinentes.

Control: Contacto con grupos de especial interés

Observación No 7

Título: No existe contacto con grupos especializados en el tema de Seguridad de Información

Norma: Se debería mantener el contacto con grupos o foros de seguridad especializados y asociaciones profesionales.

Condición: No se mantiene ninguna relación con grupos especializados en el área de Seguridad de la información

Evidencia: Cuestionario de investigación de la Seguridad de la información de FAME.

Riesgo: No se cuenta con el asesoramiento de organizaciones o grupos expertos en seguridad de la información, lo cual puede provocar rupturas en lo que respecta a la seguridad por mala administración de la misma.

Causa: No se tiene el interés de fomentar relaciones con organizaciones dedicadas a la Seguridad de Información y tampoco el conocimiento de que empresas trabajan en esa rama.

Recomendaciones: Se debería realizar la investigación sobre organizaciones o grupos especializados en seguridad de la información para mantener contacto y realizar convenios con los mismos.

Control: Revisión independiente de la seguridad de la información

Observación No 8

Título: Falta de revisión independiente de las practicas de la seguridad
De la información.

Norma: Se deberían revisar las prácticas de la institución para la gestión de la seguridad de la información y su implantación (por ej., objetivos de control, políticas, procesos y procedimientos de seguridad) de forma independiente y a intervalos planificados o cuando se produzcan cambios significativos para la seguridad de la información.

Condición: El documento que fija la política de seguridad no existe, por lo cual objetivos, políticas, procesos y procedimientos no son revisados; se realiza un análisis de posibles amenazas y contribuciones a la seguridad pero no formal es decir no es lo primordial a tomar en cuenta.

Evidencia: Cuestionario de investigación de la Seguridad de la información de FAME.

Riesgo: No se tiene el documento de política de seguridad de información, por lo cual no existe revisión periódica del mismo, no se puede dar alta ni baja ni modificaciones y tampoco saber el nivel de riesgos que se tiene a nivel empresarial.

Causa: Desconocimiento por parte de los directivos y responsables del área de tecnología en lo que respecta a Seguridad de la información.

Recomendaciones: El documento que fija la política de seguridad de la información establece la política y las responsabilidades por la seguridad de la información. Su implementación debe ser revisada independientemente para garantizar que las prácticas de la organización reflejan adecuadamente la política, y que ésta es viable y eficaz. Sin embargo esta política primero debe ser elaborada para después si poder analizarla, y mantenerla.

Objetivo de control: Terceros

Control: Identificación de los riesgos derivados del acceso de terceros

Observación No 9

Título: Falta de documentación que especifique los riesgos

Norma: Se deberían identificar los riesgos a la información de la organización y a las instalaciones del procesamiento de información de los procesos de negocio que impliquen a terceros y se deberían implementar controles apropiados antes de conceder el acceso.

Condición: El personal encargado conoce de los riesgos, manejan controles que son definidos bajo contrato pero no tienen un escrito formal el cual presente todas las posibles amenazas o riesgos presentes de que terceros tengan acceso a la Información.

Evidencia: Cuestionario de investigación de la Seguridad de la información de FAME.

Riesgo: Al momento de firmar un contrato con terceros puede no tomarse en cuenta algún riesgo por el hecho de no tenerlos presentes en un documento sino solo por conocimiento universal; esto puede provocar que no se establezcan controles adecuados los cuales accesos no autorizados a personas ajenas a la institución.

Causa: No se ha puesto interés en cuanto a documentación se refiere, obviando este tipo de situaciones, dejando vulnerable el acceso a la información.

Recomendaciones: Es necesario y obligatorio generar un documento donde se especifiquen aquellos riesgos que están presentes cuando terceros tienen acceso a nuestra información, con esto en el contrato que se haga se debe definir los controles respectivos. No se debe otorgar a terceros acceso a la información ni a las instalaciones de procesamiento de la misma hasta tanto se hayan implementado los controles apropiados y se haya firmado un contrato que defina las condiciones para la conexión o el acceso.

3.2.4.4.- Dominio: Seguridad Ligada a los Recursos Humanos

Objetivo de control: Antes del empleo

Control: Funciones y responsabilidades

Observación No 10

Título: No se ha especificado roles o responsabilidades de seguridad para los empleados

Norma: Se deberían definir y documentar los roles y responsabilidades de la seguridad de los empleados, contratistas y terceros en concordancia con la política de seguridad de la información de la organización.

Condición: No existe la política de seguridad, por lo cual no se ha definido lo roles y responsabilidades que deben cumplir los empleados en cuanto a seguridad. Si existe un control pero el mismo puede no ser el adecuado.

Evidencia: Cuestionario de investigación de la Seguridad de la información de FAME.

Riesgo: Si no existe esta política de seguridad y no se ha definido roles y responsabilidades, puede existir un alto riesgo en cuanto a lo que se refiere a robo de información, fraude, y alto riesgo de error en cuanto a procedimientos.

Causa: Como a nivel de empresa no se ha elaborado ni se ha pensado en crear el documento específico de las políticas de seguridad, entonces se presentan este tipo de amenazas.

Recomendaciones: Crear o elaborar una política de seguridad de la información en la cual se definan los roles y responsabilidades de la seguridad de los empleados, contratistas y terceros, se debe trabajar de la mano junto con

el departamento de RRHH y certificar que se emplea un proceso de verificación de antecedentes proporcional a la clasificación de seguridad de aquella información a la que va a acceder el empleado a contrata.

Objetivo de control: Durante el empleo

Control: Formación y capacitación en seguridad de la información

Observación No 11

Título: Falta de un proceso de capacitación de seguridad de la información.

Norma: Todos los empleados de la organización y donde sea relevante, contratistas y usuarios de terceros deberían recibir entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos organizacionales como sean relevantes para la función de su trabajo.

Condición: Actualmente el personal es capacitado en cuanto a Sistemas propios de la empresa más no en temas relevantes para el desempeño de sus funciones.

Evidencia: Cuestionario de investigación de la Seguridad de la información de FAME.

Riesgo: Un usuario que no esté actualizado en cuanto a políticas, y procedimientos que sean importantes para su desempeño puede convertirse en una amenaza muy alta.

Causa: No existe un procedimiento que establezca que el personal debe ser capacitado continuamente en temas que no sean sistemas informáticos de la empresa.

Recomendaciones: Se debe trabajar en modelos de capacitación en cuanto a gestión de la seguridad de la información, concienciación en seguridad de la información, seguridad y privacidad en la Web 2.0, seguridad y privacidad en comercio electrónico, etc.

Control: Proceso disciplinario

Observación No 12

Título: Falta de un proceso disciplinario para empleados.

Norma: Debería existir un proceso formal disciplinario para empleados que produzcan brechas en la seguridad.

Condición: El proceso no es documentado pero es conocimiento de todos que se presentara un aviso y después de un segundo aviso, se escalara a la gerencia.

Evidencia: Cuestionario de investigación de la Seguridad de la información de FAME.

Riesgo: Violación constante de las políticas de seguridad por parte los empleados

Causa: A nivel de empresa hay muchos procesos los cuales no se tienen documentados, entre estos procesos está el de seguir un proceso disciplinario al personal que amenace la seguridad de la información.

Recomendaciones: Debe existir un proceso disciplinario formal y escrito para los empleados que violen las políticas y procedimientos de seguridad de la institución. Dicho proceso puede servir de factor disuasivo de los empleados que, de no mediar el mismo, podrían ser proclives a pasar por alto los

procedimientos de seguridad. Asimismo, este proceso debe garantizar un trato imparcial y correcto hacia los empleados sospechosos de haber cometido violaciones graves o persistentes a la seguridad.

3.2.4.5.- Dominio: Seguridad Física y Ambiental

Objetivo de control: Áreas Seguras

Control: Perímetro de seguridad física

Observación No 13

Título: Falta de un perímetro de seguridad física para el área de sistemas.

Norma: Los perímetros de seguridad (como paredes, tarjetas de control de entrada a puertas o un puesto manual de recepción) deberían utilizarse para proteger las áreas que contengan información y recursos para su procesamiento.

Condición: FAME tienes distintos tipos de perímetros de seguridad pero la realidad no son muy seguros; existen dentro de las instalaciones pre salas que aseguran el acceso a lugares sensibles de información pero por lo demás no hay mayor seguridad, No se dispone de controles de acceso automatizados, a nivel de seguridad del personal, no se dispone de puertas ni vías contra incendio, no se tiene advertido al personal tampoco en caso de que algún fenómeno ocurra; no hay información sino solo la básica que toda persona posee.

Evidencia: Cuestionario de investigación de la seguridad de la información de FAME.

Riesgo: Ingreso no autorizado a lugares sensibles; Existe mucho peligro en cuanto al personal al momento de que se produzca un incendio o inundación ya que desconocen el procedimiento a seguir, además la información puede perderse en un abrir y cerrar de ojos debido a que la mayoría de seguridades está basada en una puerta de madera.

Causa: Al parecer no se toma en consideración lo importante de situar o localizar las áreas sensibles de información dentro de un perímetro totalmente sellado y que tenga las seguridades necesarias para no perderlas ante cualquier fenómeno que se pueda producir.

Recomendaciones: Las institución debe utilizar perímetros de seguridad para proteger las áreas que contienen instalaciones de procesamiento de información. Un perímetro de seguridad es algo delimitado por una barrera, por ejemplo. Una pared, una puerta de acceso controlado por tarjeta o un escritorio u oficina de recepción atendidos por personas. El emplazamiento y la fortaleza de cada barrera dependerán de los resultados de una evaluación de riesgos. Todas las puertas de incendio de un perímetro de seguridad deben tener alarma y cerrarse automáticamente.

Control: Controles físicos de entrada

Observación No 14

Título: Falta de controles automatizados de entrada para lugares específicos.

Norma: Las áreas de seguridad deberían estar protegidas por controles de entrada adecuados que garanticen el acceso únicamente al personal autorizado.

Condición: Existe el control de acceso en la entrada de la empresa, la cual es mediante guardias, pero para el resto de áreas no existe la seguridad necesaria. No se dispone de accesos automatizados, como tarjetas, sistemas biométricos, etc.

El mismo hecho de no tener sistemas automatizados permite que no se haga seguimiento de los accesos al personal de adentro o afuera.

Evidencia: Cuestionario de investigación de la Seguridad de la información de FAME.

Riesgo: Ingreso no autorizado a las áreas sensibles.

Causa: Se considera las áreas de tratamiento de información como sensibles pero no se toman las medidas necesarias para contrarrestar cualquier peligro.

Recomendaciones: Las áreas protegidas deben ser resguardadas por adecuados controles de acceso que permitan garantizar que sólo se permite el acceso de personal autorizado. Se debe requerir que todo el personal exhiba alguna forma de identificación visible y se lo debe alentar a cuestionar la presencia de desconocidos no escoltados y a cualquier persona que no exhiba una identificación visible.

Así como también se deberá verificar periódicamente si el personal tiene los permisos de acceso físico adecuados

Control: Seguridad de oficinas, despachos e instalaciones

Observación No 15

Título: Falta de seguridad en oficinas, despachos e instalaciones clave.

Norma: Se debería asignar y aplicar la seguridad física para oficinas, despachos y recursos.

Condición: Las oficinas así como las instalaciones clave no tienen la debida seguridad. La única seguridad con la que cuentan es que están cerradas con llave, además que no se tiene una distribución dentro de oficinas que permita tener seguridad en caso de incendios, inundaciones, etc.

Evidencia: Cuestionario de investigación de la Seguridad de la información de FAME.

Riesgo: Ingreso no autorizado a oficinas, despachos e instalaciones clave.

Causa: Se asume que con la seguridad actual que realmente no es segura se tiene todo protegido, por lo cual no se toma como idea a ejecutar.

Recomendaciones: Para la selección y el diseño de un área protegida se debe tener en cuenta la posibilidad de daño producido por incendio, inundación, explosión, agitación civil, y otras formas de desastres naturales o provocados por el hombre, actualmente el departamento de seguridad industrial está trabajando en mejoras . También deben tomarse en cuenta las disposiciones y normas en materia de sanidad y seguridad. Las instalaciones clave deben ubicarse en lugares a los cuales no pueda acceder el público.

Objetivo de control: Seguridad de los Equipos

Control: Instalación y protección de equipos

Observación No 16

Título: Falta de conocimiento del personal en cuanto a cómo actuar cerca de equipos informáticos.

Norma: El equipo debería situarse y protegerse para reducir el riesgo de materialización de las amenazas del entorno, así como las oportunidades de acceso no autorizado

Condición: Actualmente el personal desconoce los riesgos de comer, beber, fumar cerca de equipos informáticos.

Por otro lado no se ha tomado en cuenta que riesgos se tienen en caso de que un eventual desastre tenga lugar en zonas próximas a la sede de la organización

Evidencia: Cuestionario de investigación de la Seguridad de la información de FAME.

Riesgo: Se pueden producir accidentes que afecten al personal; pueden ocurrir daños en los equipos; y podría llegar a perderse todo ya que no se tiene en cuenta que no se tiene desarrollado un plan de prevención y plan de evacuación en lo que respecta a desastres en lugares próximos a la empresa.

Causa: Todavía no se llega en cuanto a seguridad del personal, física y de información al nivel que se debería y no se dan las medidas adecuadas.

Recomendaciones: Se debe tomar muy en cuenta los lugares donde se sitúan los equipos, así como capacitar al personal en lo que respecta a cómo actuar cuando se tiene un equipo informático o tecnológico a cargo.

Las instalaciones de procesamiento de información deben estar en lugares donde no se necesite mucha supervisión ya que se tiene previos controles.

Se debe tomar en cuenta el hecho de monitorear las condiciones ambientales o meteorológicas para determinar que no existan riesgos en cuanto a las instalaciones; por último se debe trabajar en un plan de salvaguardas y evacuación los cuales dicten el procedimiento a seguir en caso de que algo suceda en instalaciones próximas a la empresa.

Control: Seguridad del cableado

Observación No 16

Título: Falta de protección del cableado en ciertas áreas.

Norma: Se debería proteger el cableado de energía y de telecomunicaciones que transporten datos o soporten servicios de información contra posibles interceptaciones o daños.

Condición: Se protege el cableado entre edificios, el cableado de datos es subterráneo en algunos trayectos pero el cableado eléctrico es aéreo y no se tiene la debida protección.

Evidencia: Cuestionario de investigación de la Seguridad de la información de FAME.

Riesgo: Manipulación y daño del cableado o conexión de dispositivos no autorizados a l cableado eléctrico y de datos.

Causa: No se ha realizado un barrido para determinar los trayectos vulnerables.

Recomendaciones: El cableado debe estar protegido contra interceptación no autorizada o daño, por ejemplo mediante el uso de conductos o evitando

trayectos que atraviesen áreas públicas. Instalación de conductos blindados y recintos o cajas con cerradura en los puntos terminales y de inspección. Además, iniciar barridos para eliminar dispositivos no autorizados conectados a los cables.

Control: Retirada de materiales propiedad de la institución

Observación No 17

Título: Falta de autorización para el retiro de bienes de la institución.

Norma: No deberían sacarse equipos, información o software fuera del local sin una autorización.

Condición: No se tiene el control de revisar o monitorear si los equipos no han sido extraídos de la empresa.

Evidencia: Cuestionario de investigación de la Seguridad de la información de FAME.

Riesgo: Fuga y manipulación de la información de la institución, así como perdida de equipos que pueden o no ser costosos a nivel económico pero un bien siempre equivale a costo para una empresa.

Causa: La carencia de chequeos para detectar el retiro no autorizado de bienes de la institución.

Recomendaciones: Se pueden realizar chequeos inesperados para detectar el retiro de propiedad, dispositivos de grabación no-autorizados, armas, etc., y evitar su ingreso a la institución.

3.2.4.6.- Dominio: Gestión de Comunicaciones y Operaciones

Objetivo de control: Responsabilidades y procedimientos de operación

Control: Documentación de los procedimientos de operación

Observación No 18

Título: Inexistencia de documentación y mantenimiento continúo respecto a los procesos de operación de la institución.

Norma: Se deberían documentar y mantener los procedimientos de operación y ponerlos a disposición de todos los usuarios que lo necesiten.

Condición: La institución al momento se encuentra en actualización de procesos y procedimientos, no existe un proceso referente a los requerimientos de programación incluyendo interdependencias con otros sistemas, tiempos de inicio y terminación de tareas. Se cuenta con distintos de niveles de soporte internos y externos; y en cuanto a procedimientos de recuperación de fallos del sistema no existen normas.

Evidencia: Cuestionario de investigación de la Seguridad de la información de FAME.

Riesgo: Desconocimiento del personal en cuanto a procedimientos operativos, Así como Cese del funcionamiento de los sistemas críticos de la institución sin tener ningún tipo de reacción, ah no ser que sea el propio proveedor el que solucione el problema.

Causa: Así como otros puntos, muchos procedimientos y procesos solo son conocidos de manera universal mas no están por escrito dentro de la organización, por otro lado no existen las normas y controles en cuanto a

mantenimiento de procedimientos se refiere y por ultimo no se ha tomado en cuenta gestionar las medidas necesarias para sobre llevar un cese de funcionamiento de los aplicativos

Recomendaciones: Se recomienda documentar y mantener procedimientos de operación identificados por su política de seguridad. Los procedimientos operativos deben ser tratados como documentos formales y los cambios deben ser autorizados por el nivel gerencial.

Estos procedimientos deben especificar las instrucciones para la ejecución detallada de cada tarea y de ser posible también es recomendable preparar documentación sobre procedimientos referidos a actividades de mantenimiento de los sistemas.

Control: Separación de los recursos de desarrollo, prueba y operación

Observación No 19

Título: Falta de documentación formal que especifique los pasos a seguir para pasar de un estado de desarrollo a aun estado de implementación.

Norma: La separación de los recursos para el desarrollo, prueba y producción es importante para reducir los riesgos de un acceso no autorizado o de cambios al sistema operacional.

Condición: Al momento los recursos se encuentran separados en capas y su acceso está establecido y uso se encuentra establecido, pero lo que no sucede es que se tenga una documento formal que contenga las reglas a seguir para pasar transferir un software del estado de desarrollo a l estado implementación, además la empresa no dispone de departamento de desarrollo, por lo cual

accesos tanto al sistema como a la información la dispone el proveedor claro está sin ningún tipo de restricción mas solo la firma de confidencialidad.

Evidencia: Cuestionario de investigación de la Seguridad de la información de FAME.

Riesgo: No existe el documento que dicte que el sistema está listo para poder ser implementado, las pruebas son hechas por el mismo personal lo cual no permite un análisis completo, no existe personal que sea experto en pruebas de funcionalidad y esto puede producir que los programas no funcionen correctamente y no se definan errores, vulnerabilidades, etc.

Salida o fuga de información por medio de los proveedores, ya que tienen todo el acceso sin ningún tipo de restricción.

Causa: No se ha pensado en generar un documento ya que el desarrollo lo lleva por completo el proveedor; no se ha tomado en cuenta tampoco que el hecho de no tener un equipo de desarrollo puede traer menos riesgos a la empresa que trabajar únicamente con los proveedores.

Recomendaciones: Se recomienda trabajar con un equipo experto en QA que sea interno de la empresa, generar el documento necesario que permita establecer o no si un sistema está listo para ser implementado por ultimo es necesario de alguna manera restringir el acceso a los sistemas operativos al personal de desarrollo externo.

Objetivo de control: Gestión de la provisión de servicios por terceros

Control: Gestión de cambios en los servicios prestados por terceros

Observación No 19

Título: Inexistencia de un manejo o gestión de los cambios en la provisión de servicios prestados por terceros.

Norma: Se deberían gestionar los cambios en la provisión del servicio, incluyendo mantenimiento y mejoras en las políticas de seguridad de información existentes, en los procedimientos y los controles teniendo en cuenta la importancia de los sistemas y procesos involucrados del negocio, así como la reevaluación de los riesgos.

Condición: La empresa no dispone de una política de seguridad de información, por lo cual se desconoce de la gestión de cambios con terceros; esto provoca también que no se pueda dar mantenimiento a la misma, evitando que se puedan mejorar y revisar reglas y controles.

Evidencia: Cuestionario de investigación de la Seguridad de la información de FAME.

Riesgo: Compromiso, daño o pérdida de recursos de información.

Causa: Desconocimiento de los riesgos de la provisión de servicios de terceros sin una supervisión permanente de los mismos y sus cambios.

Recomendaciones: Es recomendable supervisar los cambios que realizan terceros en los servicios que brindan a la institución con el fin de que la seguridad no se vea comprometida de alguna manera por dichos cambios.

Objetivo de control: Planificación y aceptación del sistema

Control: Gestión de capacidades

Observación No 20

Título: Inexistencia de proyecciones de las capacidades que requerirán los sistemas en el futuro para su correcto funcionamiento.

Norma: Se debería monitorizar el uso de recursos, así como de las proyecciones de los requisitos de las capacidades adecuadas para el futuro con objeto de asegurar el funcionamiento requerido del sistema.

Condición: No se realiza proyecciones acerca de los requerimientos futuros de los sistemas, ya que se trabaja con lo que se tiene sin pensar en posibles cambios para mejora.

Evidencia: Cuestionario de investigación de la Seguridad de la información de FAME.

Riesgo: Desactualización en los sistemas para manejar nuevos escenarios por lo tanto posibles fallos, que comprometan las actividades críticas de la organización.

Causa: Falta de conocimiento acerca de la importancia de hacer proyecciones de los requerimientos de las capacidades de los sistemas.

Recomendaciones: Se recomienda realizar proyecciones de los futuros requerimientos de capacidad de los sistemas, estas proyecciones deben tomar en cuenta los nuevos requerimientos de negocios y sistemas y las tendencias actuales y proyectadas en el procesamiento de la información de la institución.

Objetivo de control: Protección contra código malicioso y descargable

Control: Controles contra el código malicioso

Observación No 21

Título: Falta de concientización de los usuarios en cuantos a software malicioso.

Norma: Se deberían implantar controles de detección, prevención y recuperación contra el software malicioso, junto a procedimientos adecuados para la concienciación de los usuarios.

Condición: La empresa cuenta con restricciones y controles en cuanto a la instalación de código malicioso y prevención contra el mismo en ejecución, pero lo que no se tiene es concientización por parte de los usuarios para contrarrestar por completo esta amenaza.

Evidencia: Cuestionario de investigación de la Seguridad de la información de FAME.

Riesgo: Infección de los sistemas operativos, divulgación de información, etc.

Causa: Desconocimiento por parte de los usuarios en cuanto a lo que es y lo que puede causar la instalación de software malicioso, así como también desconocimiento para saber diferenciar que es y que no es software malicioso.

Recomendaciones: Es recomendable entrenar al personal para que sepan diferenciar si una aplicación puede ser una amenaza así como también hacer entender el problema y la gravedad de la existencia de virus y software malicioso instalado en los sistemas de la empresa.

Control: Controles contra el código descargado en el cliente (móvil)

Observación No 22

Título: Inexistencia de un procedimiento sobre la utilización de código móvil.

Norma: Cuando se autoriza la utilización de código móvil, la configuración debería asegurar que dicho código móvil opera de acuerdo a una política de seguridad definida y se debería evitar la ejecución de los códigos móviles no autorizados.

Condición: No existe un procedimiento formal el cual establezca el uso de código móvil, y tomando en cuenta que no existe una política de seguridad, entonces no se puede trabajar en controles adecuados.

Evidencia: Cuestionario de investigación de la Seguridad de la información de FAME.

Riesgo: Ejecución de aplicaciones transferidas de un equipo a otro las cuales atenten contra la seguridad.

Causa: Desconocimiento del riesgo que implica la utilización no autorizada de código móvil, y no se ha tomado en cuenta como riesgo relevante para la empresa.

Recomendaciones: Se recomienda adoptar una política formal que tome en cuenta los riesgos que implica trabajar con aplicaciones que puedan transferirse de un equipo a otro y se ejecuten sin ningún control.

Objetivo de control: Manipulación de los soportes

Control: Gestión de soportes extraíbles

Observación No 23

Título: Inexistencia de reglas en cuanto al uso de medios removibles.

Norma: Se deberían establecer procedimientos para la gestión de los medios informáticos removibles.

Condición: No existen reglas, por lo tanto no hay control sobre el uso de medios removibles o extraíbles, estos pueden ser utilizados sin ninguna restricción.

Evidencia: Cuestionario de investigación de la Seguridad de la información de FAME.

Riesgo: Daño, robo, pérdida o acceso no autorizado a la información critica de la institución.

Causa: No se toma este factor como una amenaza a la información y sistemas de la empresa, por desconocimiento ante el hecho de establecer procedimientos que regulen el uso de dispositivos removibles.

Recomendaciones: Se recomienda supervisar de forma regular el cumplimiento y la actualización de los procedimientos para la gestión de los medios informáticos removibles y se debe realizar un registro de todos los retiros de dichos medios a fin de mantener una pista de auditoría.

Control: Procedimientos de manipulación de la información

Observación No 24

Título: Falta de un procedimiento especifico que establezca las tareas a seguir en cuanto a manipulación y almacenamiento de información.

Norma: Se deberían establecer procedimientos para la manipulación y almacenamiento de la información con el objeto de proteger esta información contra divulgaciones o usos no autorizados o inadecuados.

Condición: Existen controles para lo que respecta a manipulación y almacenamiento de información, pero lamentablemente así como otros procedimientos, este también es solo conocido levemente mas no lo existe documentado y formal.

Evidencia: Cuestionario de investigación de la Seguridad de la información de FAME.

Riesgo: Divulgaciones y usos no autorizados o inadecuados de cualquier tipo de información.

Causa: No se ha da importancia al hecho de tener documentado todo tipo de proceso y procedimiento el cual amenace contra la seguridad de la información.

Recomendaciones: Es recomendable definir cuáles son los procedimientos que los usuarios deben seguir. Hay que tener en cuenta que los procedimientos de manejo de información deben elaborarse según la clasificación de la misma dentro de la institución.

Control: Seguridad de la documentación de sistemas

Observación No 25

Título: Falta de seguridad en cuanto a la documentación de los sistemas.

Norma: Se debería proteger la documentación de los sistemas contra accesos no autorizados.

Condición: Actualmente la documentación de los sistemas se encuentra archivada en estantes los cuales no son seguros.

Evidencia: Cuestionario de investigación de la Seguridad de la información de FAME.

Riesgo: Perdida de documentación relevante en cuanto a los sistemas, puede llegarse a conocer las vulnerabilidades de los mismos y esto en manos no adecuadas puede llegar a convertirse en una amenaza muy alta.

Causa: No se ha dado mayor importancia al hecho de almacenar de manera segura la documentación de los sistemas que la empresa actualmente posee y desconocimiento por parte del personal encargado en cuanto al hecho de saber qué tipo de amenazas se pueden presentar.

Recomendaciones: Se recomienda tener la documentación referente a los sistemas informáticos y aplicativos sino es en caja fuerte, en lugar donde se tenga el mínimo acceso del personal, es decir que se tengan algunos filtros de seguridad los cuales permitan bloquear cualquier tipo de acceso y toma de documentación no autorizada.

Objetivo de control: Intercambio de información

Control: Políticas y procedimientos de intercambio de información

Observación No 26

Título: Falta de políticas y procedimientos documentados formalmente para proteger el intercambio de información través de servicios de comunicación.

Norma: Se deberían establecer políticas, procedimientos y controles formales de intercambio con objeto de proteger la información mediante el uso de todo tipo de servicios de comunicación.

Condición: No existen políticas, procedimientos formales, controles si existen pero no documentados.

Evidencia: Cuestionario de investigación de la Seguridad de la información de FAME.

Riesgo: Pérdida o uso inadecuado de la información que intercambia la institución con otras organizaciones e internamente.

Causa: Desconocimiento de los riesgos que implica el intercambio de información con otras organizaciones sin el debido control en la seguridad.

Recomendaciones: Se recomienda establecer acuerdos, algunos de los cuales pueden ser formales, incluyendo los acuerdos de custodia de software cuando corresponda, para el intercambio de información y software entre organizaciones. Las especificaciones de seguridad de los acuerdos de esta índole deben reflejar el grado de sensibilidad de la información involucrada.

Control: Soportes físicos en transito

Observación No 27

Título: Falta de protección de los medios físicos y de información mientras se encuentran en tránsito.

Norma: Se deberían proteger los medios que contienen información contra acceso no autorizado, mal uso o corrupción durante el transporte fuera de los límites físicos de la organización.

Condición: Si la información es requerida entre sucursales u oficinas, se trata de que la gerencia sea la autorizada de pedirla, pero ni la información que viaja como los medios físicos que la transportan, tienen algún tipo de seguridad contra perdida o caída.

Evidencia: Cuestionario de investigación de la Seguridad de la información de FAME.

Riesgo: Perdida de información, daño en los dispositivos, accesos no autorizados, mal uso o corrupción de la información durante el transporte fuera de los límites físicos de la institución.

Causa: No se ha puesto en marcha ningún plan que permita proteger a la empresa de estos posibles daños, por falta de interés, desconocimiento o simplemente no tomarlo como un hecho que ponga en riesgo la información de la organización.

Recomendaciones: Se recomienda el uso de medios de transporte o servicios de mensajería confiables. Además es necesario acordar con las autoridades una lista de servicios de mensajería autorizados e implementar un procedimiento para verificar la identificación de los mismos. El embalaje debe

ser suficiente para proteger el contenido contra daños durante el tránsito y si fuera el caso seguir las especificaciones de los fabricantes o proveedores.

Se recomienda también manejar aplicaciones las cuales resguarden la información mediante claves para que así, en caso de pérdida, o robo, la misma no pueda ser difundida o divulgada.

Control: Sistemas de información empresariales

Observación No 28

Título: Inexistencia de documentación formal que describa el proceso y procedimientos.

Norma: Se deberían desarrollar e implementar políticas y procedimientos con el fin de proteger la información asociada con la interconexión de sistemas de información del negocio.

Condición: No se tiene documentado formalmente políticas o procedimientos que establezcan la protección de la información asociada con la interconexión de los sistemas existentes.

Evidencia: Cuestionario de investigación de la Seguridad de la información de FAME.

Riesgo: Desconocimiento del personal, perdida de información o uso no autorizado de la misma.

Causa: Existe interconexión entre sistemas que la empresa maneja, el personal conoce de los riesgos que se pueden presentar pero no se tiene documentado formalmente los controles y las políticas a seguir ante cualquier amenaza a la seguridad de la información.

Recomendaciones: Es recomendable tener documentado formalmente las políticas y procedimientos a seguir para proteger la información asociada con la interconexión de los sistemas de la empresa.

Objetivo de control: Supervisión

Control: Sincronización del reloj

Observación No 29

Título: Inexistencia de un proceso de sincronización de relojes de los sistemas de procesamiento de información.

Norma: Se deberían sincronizar los relojes de todos los sistemas de procesamiento de información dentro de la organización o en el dominio de seguridad, con una fuente acordada y exacta de tiempo.

Condición: Cada sistema trabaja con su fecha y hora locales, se asume están sincronizadas pero no existe un procedimiento el cual establezca centralizar el control de la fecha y hora, tampoco un control y monitores sobre cada uno de los servidores.

Evidencia: Cuestionario de investigación de la Seguridad de la información de FAME.

Riesgo: Transacciones con fecha y horas no reales, las cuales pueden provocar corrupción en la información almacenada en las bases de datos, entorpecimiento en las investigaciones en casos legales o disciplinarios y daños en la credibilidad de la evidencia.

Causa: Desconocimiento de la importancia de la sincronización de los relojes y/o falta de interés en tener una única fuente.

Recomendaciones: La correcta configuración de los relojes de las computadoras o servidores es recomendable para garantizar la exactitud de los registros de auditoría, que pueden requerirse para investigaciones.

3.2.4.7.- Dominio: Control de Acceso

Objetivo de control: Requerimientos de negocio para el control de accesos

Control: Política de control de accesos

Observación No 30

Título: Falta de una política de control de accesos

Norma: Se debería establecer, documentar y revisar una política de control de accesos en base a las necesidades de seguridad y de negocio de la organización.

Condición: Actualmente no se dispone de una política documentada referente al control de accesos del personal a los sistemas; cada sistema tiene sus reglas establecidas pero no hay una política a nivel empresarial.

Evidencia: Cuestionario de investigación de la Seguridad de la información de FAME.

Riesgo: Acceso no autorizado a los sistemas, mal manejo de los módulos de seguridad.

Causa: No se ha tomado como idea documentar una política la cual rija sobre el control de accesos basado en la seguridad de la información.

Recomendaciones: Se recomienda al nivel gerencial crear, definir y difundir una política que gestione el control de accesos, basado en la seguridad de la empresa y de acuerdo al giro de negocio.

Objetivo de control: Gestión de acceso de usuario

Control: Revisión de los derechos de acceso de los usuarios.

Observación No 31

Título: Falta de seguimiento y monitoreo en cuanto a privilegios de acceso de los usuarios a los sistemas.

Norma: El órgano de Dirección debería revisar con regularidad los derechos de acceso de los usuarios, siguiendo un procedimiento formal.

Condición: Se realiza un análisis de derechos de acceso de los usuarios cuando algo se suscita, mas no se da una revisión regular.

Evidencia: Cuestionario de investigación de la Seguridad de la información de FAME.

Riesgo: Acceso no autorizado a los sistemas.

Causa: Se asume que todos los privilegios de acceso de los usuarios son los indicados, por lo cual no se hace un seguimiento.

Recomendaciones: Es recomendable que los directivos, o persona designada como responsable realice un chequeo de los privilegios o derechos de acceso que tienen los usuarios sobre los sistemas y así no esperar a que un acceso no autorizado se presente.

Objetivo de control: Control de acceso al sistema operativo

Control: Sistema de gestión de contraseñas.

Observación No 32

Título: No se garantiza la calidad de las contraseñas de los usuarios.

Norma: Los sistemas de gestión de contraseñas deberían ser interactivos y garantizar la calidad de las contraseñas.

Condición: Actualmente las contraseñas son manejadas por los propios usuarios, si bien es cierto se tiene la enseñanza de buenas prácticas, los usuarios tienen la libertad de escoger sus credenciales y no se tiene control para garantizar las mismas.

Evidencia: Cuestionario de investigación de la Seguridad de la información de FAME.

Riesgo: Fraude en cuanto a contraseñas, y accesos no autorizados.

Causa: No se ha establecido una política la cual establezca que se certifiquen o garanticen las contraseñas creadas por los usuarios.

Recomendaciones: Dentro de los sistemas de gestión de contraseñas es recomendable que se usen políticas las cuales vayan de la mano con las buenas prácticas de uso y selección de contraseñas.

Control: Desconexión automática de terminales.

Observación No 33

Título: Falta de una política que permita la desconexión automática de la sesión de usuarios.

Norma: Se deberían desconectar las sesiones tras un determinado periodo de inactividad.

Condición: Se tiene definidas políticas de cierre de sesión dentro de las aplicaciones mas no a nivel de dominio, es decir la sesión de usuario dentro del sistema operativo no tiene ninguna política definida que genere la desconexión automática después de cierto tiempo de inactividad.

Evidencia: Cuestionario de investigación de la Seguridad de la información de FAME.

Riesgo: Acceso no autorizado al sistema operativo.

Causa: No se ha tomado este punto como una posible amenaza, es por esto que solo a nivel de los sistemas existe la regla.

Recomendaciones: Es recomendable generar una política dentro de los perfiles de usuario existentes en el dominio de la empresa la cual produzca el cierre de sesión a nivel de sistema operativo tras cierto tiempo de inactividad.

3.2.4.8.- Dominio: Adquisición, desarrollo y mantenimiento de los sistemas de información

Objetivo de control: Seguridad de las aplicaciones del sistema.

Control: Control del proceso interno.

Observación No 34

Título: Falta de chequeos o validación de la información tratada en las aplicaciones.

Norma: Se deberían incluir chequeos de validación en las aplicaciones para la detección de una posible corrupción en la información debida a errores de procesamiento o de acciones deliberadas.

Condición: Actualmente no se realiza ningún tipo de chequeo o validación de la información tratada por las aplicaciones, para poder determinar si existe corrupción en los datos, la gestión se realiza únicamente cuando se presenta alguna excepción.

Evidencia: Cuestionario de investigación de la Seguridad de la información de FAME.

Riesgo: Perdida de integridad de la información, perdida de información debido a corrupción de datos.

Causa: Se asume que las aplicaciones trabajan sin problemas por que en cierto momento se hicieron las pruebas adecuadas, por lo tanto no se realiza seguimiento o no se realizan validaciones de la información que se encuentra en los sistemas.

Recomendaciones: Se recomienda poner dentro la planificación del departamento de sistemas, una tarea mensual la cual consista en hacer un barrido de los datos tratados en los aplicativos y determinar si son correctos y validos.

Si no se tiene un equipo de desarrollo y los aplicativos son externos es decir adquiridos mediante proveedor, entonces se deberá plantear de manera correcta que tipo de validación de datos se necesita en los aplicativos en cuanto a entradas se refiere.

Objetivo de control: Controles criptográficos.

Control: Política de uso de los controles criptográficos.

Observación No 35

Título: Inexistencia de una política formal y escrita la cual establezca el uso de controles criptográficos.

Norma: Se debería desarrollar e implantar una política de uso de controles criptográficos para la protección de la información.

Condición: No se ha definido una política de uso de controles criptográficos, si los aplicativos con los que la empresa trabaja tienen métodos criptográficos en buena hora.

Evidencia: Cuestionario de investigación de la Seguridad de la información de FAME.

Riesgo: Con un acceso no autorizado a la información almacenada en la Base de Datos o archivos planos que los aplicativos manejen, se puede obtener sin mayor dificultad toda la información.

Causa: No se ha puesto mayor interés en cuanto a seguridades de los aplicativos, se ha establecido seguridades en cuanto a gestión de identidad pero no se ha puesto interés en desarrollar una política la cual obligue a manejar controles criptográficos.

Recomendaciones: Debido a las amenazas informáticas que en la actualidad las empresas afrontan cada vez es más seguro establecer políticas que obliguen a los aplicativos a trabajar con controles criptográficos para que así la información no pueda ser divulgada fácilmente.

Control: Cifrado.

Observación No 36

Título: Falta de gestión en cuanto al uso de claves con técnicas criptográficas.

Norma: Se debería establecer una gestión de las claves que respalde el uso de las técnicas criptográficas en la organización.

Condición: Actualmente ciertos aplicativos que la empresa dispone manejan técnicas criptográficas en cuanto a claves de acceso se refiere.

Evidencia: Cuestionario de investigación de la Seguridad de la información de FAME.

Riesgo: Al igual que la información, las claves de acceso de los usuarios pueden ser descubiertas mediante accesos no autorizados y si las mismas no son tratadas mediante técnicas criptográficas, es decir no tienen ningún tipo de cifrado, podrían ser tratadas sin necesidad de procedimientos adicionales y utilizadas sin problema poniendo en riesgo a toda la información de la empresa.

Causa: Por el mismo hecho de no existir una política la cual obligue a manejar controles criptográficos sobre la información en los sistemas, pues no existe la gestión necesaria en cuanto al manejo de claves de acceso usando técnicas criptográficas.

Recomendaciones: Se recomienda establecer una gestión de las claves que respalde el uso de las técnicas criptográficas en la organización, mediante software incluso gratuitos que al momento existen.

Objetivo de control: Seguridad de los ficheros del sistema.

Control: Protección de los datos de prueba del sistema.

Observación No 37

Título: Falta de control sobre la base de información sobre la cual se realizan las pruebas de los sistemas.

Norma: Se deberían seleccionar, proteger y controlar cuidadosamente los datos utilizados para las pruebas.

Condición: La empresa tiene la infraestructura para realizar pruebas totalmente apartado del ambiente de producción, pero cuando se ingresa o se trabaja con el ambiente de pruebas, la información que es usada son bases de datos de la empresa, a la cual se tiene acceso por parte de externos.

Evidencia: Cuestionario de investigación de la Seguridad de la información de FAME.

Riesgo: Fuga de información, al exterior de la empresa sin necesidad de connivencia interna.

Causa: No se toma como una amenaza el estar en ambiente de pruebas con personal externo a la organización y trabajar con la información real de la empresa.

Recomendaciones: Es necesario que para ambientes de pruebas, la información no sean las bases de datos de la organización, que el ingreso de datos y tratamiento de información sea real si pero que la base de información no sea la que la empresa maneja.

3.2.4.9.- Dominio: Gestión de continuidad del negocio

Todo este dominio posee problemas debido a que no se ha implementado un plan de continuidad, al momento se encuentra en desarrollo.

Observación No 38

Título: Inexistencia de un plan de continuidad del negocio.

Norma: Reaccionar a la interrupción de actividades del negocio y proteger sus procesos críticos frente a desastres o grandes fallos de los sistemas de información.

Condición: La empresa no dispone de ningún plan o procedimientos para poder reaccionar ante interrupciones o fallos de los sistemas.

Evidencia: Cuestionario de investigación de la Seguridad de la información de FAME.

Riesgo: Cese total o parcial de las actividades críticas de la organización que represente pérdidas de cualquier índole.

Causa: La empresa se ha demorado demasiado en poner en marcha la creación de un plan de continuidad del negocio, tal vez por falta de interés, conocimiento o simplemente pensar que sus sistemas no van a fallar en ningún momento.

Recomendaciones: Se recomienda implementar un proceso controlado para el desarrollo y mantenimiento de la continuidad de los negocios en toda la organización. Este debe contemplar la identificación de riesgos que enfrenta la organización en términos de probabilidad de ocurrencia e impacto, incluyendo la identificación y priorización de los procesos críticos de los negocios, debe comprender también el impacto que una interrupción puede tener en los negocios; se recomienda además considerar la contratación de seguros que podrían formar parte del proceso de continuidad del negocio.

3.2.4.10.- Dominio: Cumplimiento

Objetivo de control: Cumplimiento de los requisitos legales

Control: Protección de datos y privacidad de la información personal.

Observación No 39

Título: Falta de responsabilidades en cuanto al resguardo de información de carácter personal.

Norma: Se debería garantizar la protección y privacidad de los datos de carácter personal según requiera la legislación, regulaciones y, si fueran aplicables, las cláusulas relevantes contractuales.

Condición: Al momento existen procesos específicos para cada departamento que garantizan la protección y privacidad de los datos personales sin embargo

no existen controles para imponer responsabilidades a aquellas personas que recopilan, procesan y divulgan información de este tipo.

Evidencia: Cuestionario de investigación de la Seguridad de la información de FAME.

Riesgo: Fuga de información de carácter personal sin posibilidad de conocimiento de la persona o personas responsables a quienes aplicar sanciones.

Causa: Desconocimiento del riesgo que representa la fuga de información personal por lo que no existe una concientización sobre la importancia del conocimiento de la legislación sobre protección de datos.

Recomendaciones: El cumplimiento de la legislación sobre protección de datos requiere una estructura y un control de gestión adecuados. Por esta razón se recomienda la designación de un responsable a cargo de la protección de datos que oriente a las autoridades, usuarios y prestadores de servicios de la institución acerca de sus responsabilidades individuales y de los procedimientos específicos que deben seguirse.

Control: Prevención del uso indebido de los recursos de tratamiento de la información.

Observación No 40

Título: Falta de monitoreo sobre el trabajo que los usuarios realizan y son ajenos al negocio de la empresa.

Norma: Se debería disuadir a los usuarios del uso de los recursos dedicados al tratamiento de la información para propósitos no autorizados.

Condición: Existen sanciones sobre las personas que realicen actividades ajenas a la empresa utilizando recursos de la misma pero no se realiza el monitoreo respectivo.

Evidencia: Cuestionario de investigación de la Seguridad de la información de FAME.

Riesgo: Uso indebido de los recursos de tratamiento de la información por falta de concientización de los usuarios.

Causa: Falta de interés por gestionar el monitoreo respectivo de las actividades realizadas por los usuarios.

Recomendaciones: La utilización de los recursos de información con propósitos no autorizados o ajenos a las actividades de la institución, sin la aprobación de la autoridad pertinente, debe ser considerada como uso indebido. Si dicha actividad es identificada mediante monitoreo u otros medios, es necesario notificar a la autoridad interesada para que se tomen las acciones disciplinarias que correspondan.

3.3.- ANÁLISIS Y EVALUACIÓN DE RIESGOS DE FAME

Para la elaboración del presente análisis de los riesgos que pueden quebrantar el desarrollo de las actividades de FAME, se ha hecho uso de la metodología MAGERIT versión 2 y su respectiva automatización con la herramienta PILAR 5.

Las fases en las que nos basamos para poder elaborar el análisis de riesgos fueron:

- Recopilación de información.
- Identificación de los activos relevantes.
- Valoración de los activos.
- Determinación de las amenazas potenciales sobre cada activo.
- Identificación del grado de vulnerabilidad de cada activo a las amenazas que le afectan.
- Estimación del impacto sobre el activo de la materialización de la amenaza.
- Medida del riesgo.

.

3.3.1.- Identificación de los activos de la organización

Tabla 3.1 Activos del complejo Fabril Fame

Activos del Complejo FABRIL FAME SA	
Servidores	Servidor De Dominio
	Servidor de Correos e Internet
	Servidor de Sistema de Nomina
	Servidor de Sistema Financiero y Contable
	Servidor transaccional y operativo BAAN
Aplicativos	Sistema encargado de nomina RRHH – ADAM
	Sistema Integrado Financiero – SIAF
	ERP – BAAN
	SO. Red Hat Linux
	SO. AIX
	SO. Windows 2003
	SO. Windows xp
	Microsoft office
	Reporteador – QLICKVIEW
	Sistema de Gestion de archivos - 9700DOC
Equipamiento	Puestos de Trabajo
	Camaras de Seguridad
	Generadores Electricos
	Equipos Multimedia
	Central Telefonica
	Proyectores Digitales
Redes	Routers
	Switchs
	Equipos de Comunicación
	Equipos de Radio
	Convertidores
	Antenas
	Access Point
Infraestructura	Oficinas
	Cuarto de Servidores
	Cableado Estructurado
	Fibra Óptica
	Alarmas
	Material y Suministros de Oficina

3.3.2.- Resultados obtenidos de la utilización de Magerit y Pilar

En base a los datos obtenidos y al análisis de la organización, se realizó una asociación de dependencias para los diferentes activos en el árbol creado. A continuación, asignando un rango de valoración de 0 a 10 para cada dimensión y activo, y considerando las relaciones de dependencia definidas con anterioridad, se construyó el Modelo de Valor.

Tomando como referencia el conjunto de amenazas previstas para cada activo por la herramienta PILAR y considerando la opinión y experiencia de los usuarios, fue posible determinar la frecuencia de materialización de una amenaza (modelada con una tasa anual de ocurrencia) y la medida de la degradación de cada activo. La información se organizó en el Mapa de Riesgos.

Una vez identificado y valorado, el primer paso para la gestión efectiva y reducción a un nivel aceptable del riesgo es la selección de salvaguardas aplicables.

Finalizado el proceso, se presenta los resultados del análisis de riesgos, los cuales se representan mediante gráficas entregadas por la herramienta.

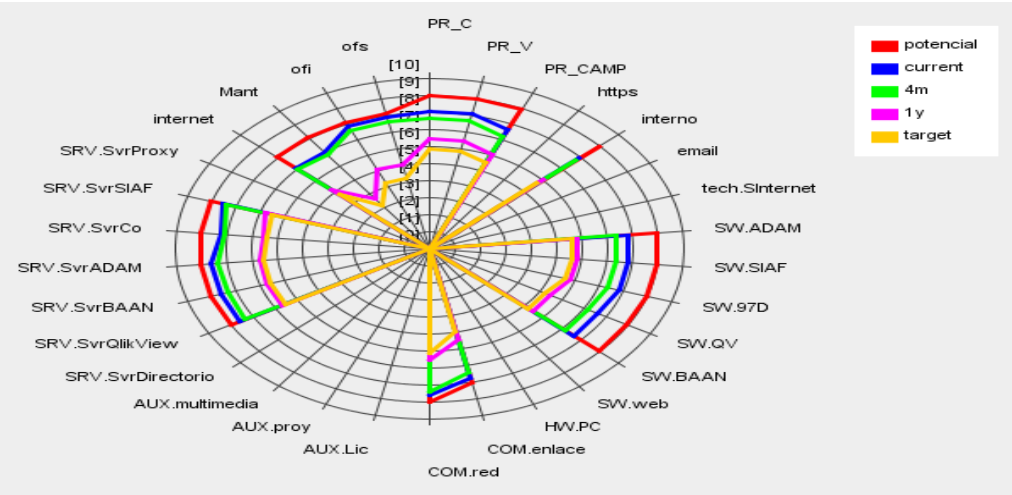


Diagrama 3.2: Riesgo Residual

De la misma manera, la herramienta utilizada nos ayuda a realizar el análisis de riesgo de acuerdo a los criterios de la norma ISO 27002, esto es de mucha ayuda ya que lo aplicado en el plan de seguridad informática es esta norma.

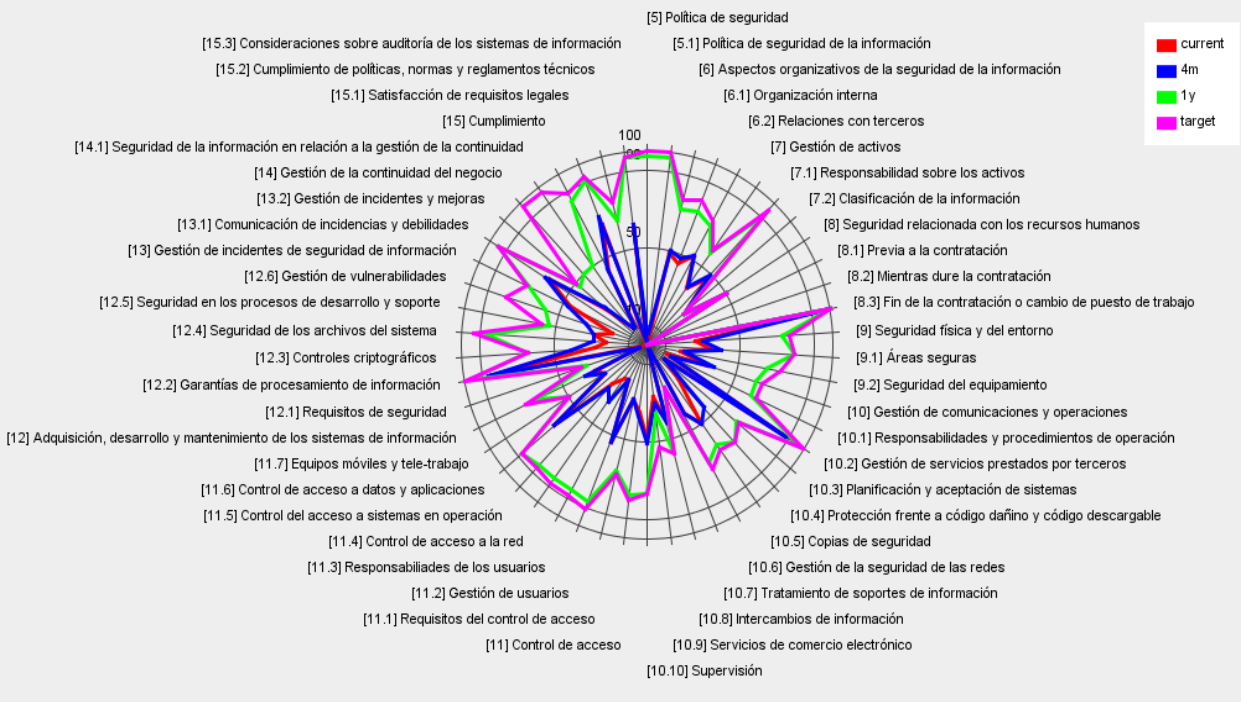


Diagrama 3.3 Análisis de Riesgos según Norma ISO 27002

CAPÍTULO IV

PLANIFICACIÓN ESTRATÉGICA DE TECNOLOGÍAS DE INFORMACIÓN

4.1.- ANÁLISIS DE LA SITUACIÓN ACTUAL

4.1.1.- Modelo Operativo

Fabril Fame, para el cumplimiento de su misión y objetivos apalanca su gestión mediante sus procesos internos de producción que se clasifican en función de su grado de contribución al cumplimiento de la misión institucional.

Departamento de Operaciones

Es el departamento encargado de la planifica y ejecución de la producción de los diferentes productos que ofrece Fame al mercado nacional e internacional. Este departamento es fundamental en la operación de la empresa para poder alcanzar los objetivos planteados.

Procesos:

- Gestión de Costos.
- Diseño.
- Mantenimiento Industrial.
- Producción de Vestuario y equipo pesado.
- Producción de Calzado.

Actividades:

- Elaboración de planes de producción de las plantas
- Recibir Órdenes de Ventas
- Generar Órdenes de Producción.
- Crear el Requerimiento de Materiales a bodegas en el sistema Baan.
- Entregar Ordenes de Producción a Control de Calidad, Logística y operarios
- Establecer estándares de cortes y molderías de materiales.
- Registrar producción diaria
- Registrar producto en reproceso.

Departamento de Comercialización

Se encarga de planificar y proyectar las ventas de acuerdo a la demanda del mercado y considerando la capacidad instalada de la planta de producción.

Procesos:

- Planificación y Proyección de Ventas.
- Ventas y Licitaciones
- Promoción y Publicidad
- Facturación.
- Crédito y Finanzas.
- Satisfacción del Cliente.

Actividades:

- Realizar una planificación y proyección de ventas
- Gestionar las ventas y licitaciones con clientes
- Realizar el cobro y efectivización de las facturas a los clientes para cumplir con los objetivos de recuperación de cartera.
- Promocionar, realizar publicidad y pautaje en medios escritos acerca de los productos y servicios que ofrece la empresa
- Garantizar a los clientes y empresa un adecuado manejo de la facturación que se realiza.
- Medir la satisfacción de los clientes en relación a los productos y servicios que la empresa entrega

Departamento de Logística

Este departamento es el encargado de planificar y proveer a la empresa de todos los materiales e insumos de materia prima o productos externos necesarios para ejecutar los planes de producción y normal cumplimiento del giro de negocio.

Procesos:

- Planificación.
- Adquisiciones.
- Calificación de Proveedores.
- Evaluación del Desempeño.

Actividades:

- Planificar el aprovisionamiento de insumos de materia prima.
- Gestionar las importaciones y/o exportaciones de productos o materia prima.
- Analizar y calificar proveedores.
- Generar Órdenes de Compra a proveedores.
- Recepcionar la mercadería.
- Ingresar la mercadería en bodega.
- Bodega realiza la distribución de materia prima según la planificación de producción.

Departamento Control de Calidad

Es el encargado de implementar y ejecutar la metodología adecuada para evaluar y determinar si la calidad de la materia prima, productos terminados y productos tercerizados, cumplen con los estándares mínimos requeridos.

Procesos:

- Control de Calidad en procesos y muestra de materia prima.
- Control de Calidad del Producto Terminado.
- Control de Calidad de Productos Tercerizados

Actividades:

- Determinar la metodología para el desarrollo del control de calidad de materias primas, producto terminado y productos tercerizados con el propósito de garantizar su correcta evaluación.

4.1.2.- Tecnologías de Información

Portafolio de Aplicaciones de software

Fame para ejecutar sus proyectos de desarrollo de Sistemas de Información lo hace con el apoyo del departamento de sistemas de Holding Dine S.A. Las aplicaciones que actualmente forman parte del portafolio de software se detallan a continuación:

- Sistema ERP BAAN
- Sistema Business Intelligence QlikView
- Sistema Strategylink
- Sistema 9000doc
- Sistema Adam V3

4.1.3.- Infraestructura Técnica (HARDWARE Y COMUNICACIONES)

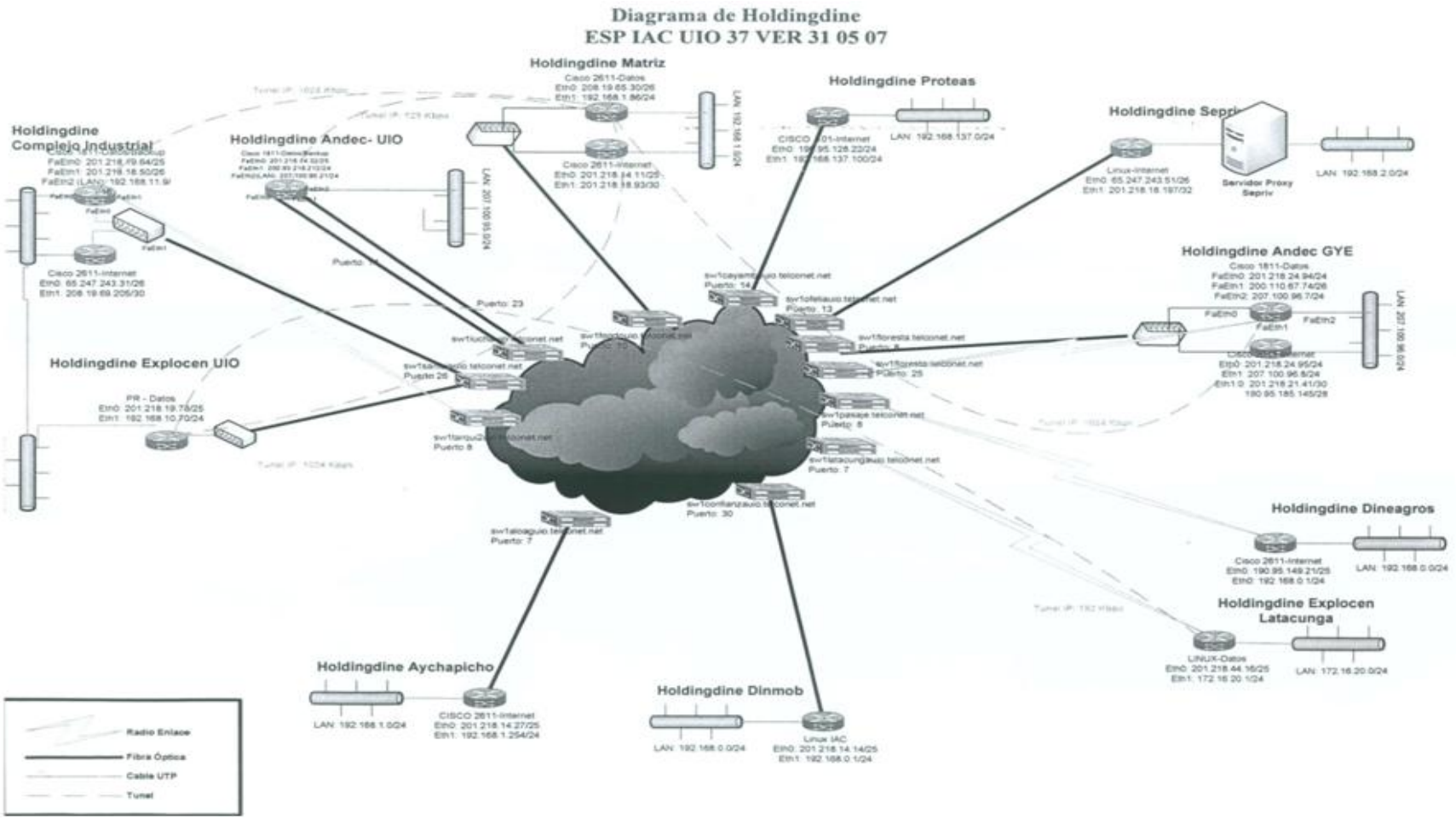


Diagrama 4.1 Red de comunicaciones FAME

4.1.4.- Conformación de la estructura de la organización de TI

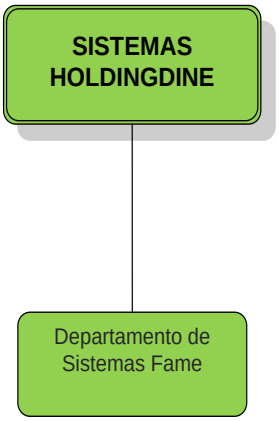


Diagrama 4.2 Estructura Organizacional TI

El departamento de sistemas de Holding Dine, asigna a un encargo de manejar el área de sistemas de Fame. El encargado coordina con dos técnicos de soporte los trabajos del área de tecnología y se encarga de encaminar los requerimientos técnicos de software o hardware para que sean atendidos por las empresas contratadas para brindar el servicio.

4.1.5.- Análisis Financiero

Tabla 4.1: Presupuesto TI 2011

Descripción	Valor ($)
EQUIPO	
Computador Personal (Pcs)	6.400
Blade de servidores	3.000
Swtich	1.500
Impresoras	2.800
Repuestos - Herramientas – Accesorios	1.000
Sistema de respaldos	3.000
Dispositivos de almacenamiento	300
TOTAL EQUIPO	**18.000**

COMUNICACIONES	
Enlace de Comunicación: Internet y Datos	1.800
Access point	250
Central Telefonía IP Complejo Holding Dine	2.000
TOTAL COMUNICACIONES	**4.050**
SOFTWARE	
Mantenimiento BAAN	2.000
Mantenimiento ADAM V3	1.125
Mantenimiento QlikView	500
Mantenimiento Asinfo	
Mantenimiento del Strategylink	500
Mantenimiento del 9000doc	
Sistema de Control documental - Correspondencia	2.000
Mantenimiento Citrix	
Renovación Software Antivirus	2.400
Renovación de Consola Antivirus	300
Proyecto ITC	30.000
TOTAL SOFTWARE	**38.825**
TOTAL DE TECNOLOGÍA DE LA INFORMACIÓN	**60.875**

El presupuesto asignado para TI en el año 2011, corresponde al 7% del presupuesto general, teniendo como gran parte del presupuesto al proyecto Común de Telecomunicaciones.

Con respecto al presupuesto para mantenimientos de Software, se evidencia un gasto racional teniendo en cuenta el portafolio de aplicaciones, con un promedio de $6000 anuales, correspondiente al 10% del presupuesto de TI.

Para este año se asigna un rubro de $3000 para un sistema de respaldos que es importante para salvaguardar la información de la empresa.

4.2.- MODELO DE LA ORGANIZACIÓN

4.2.1.- Análisis del entorno

Este análisis indica que se debe realizar un BENCHMARKING, con el estado de los indicadores en el mercado de los entes relacionados a la industria textil y de relación indirecto por lo que se lo realizará con respecto a los siguientes puntos:

Tabla 4.2: Análisis Clientes

Interés / requerimiento	Problema Percibido
Calidad: durabilidad, comodidad en el uso, diseños actuales (moda), tallas y diseño adecuadas.	Diseños no actuales, calzado incomodo, no hay tallas de acuerdo a los estándares, problemas en moldería.
Precios accesibles	Precios altos en algunos productos
Entrega oportuna	Tiempos de entrega muy amplios y falta de cumplimiento de tiempos acordados
Accesibilidad y disponibilidad del producto	Falta de canales de distribución y disponibilidad de productos
Descuentos y facilidades de pago	Restringidos descuentos y facilidades de pagos

Tabla 4.3: Análisis Competidores

Interés / requerimiento	Problema percibido
Ingresar al mercado militar	Competencia con precios más bajos, empresas de tipo artesanal.
Incrementar margen de ganancia	Restricción en compra de materias primas, baja calidad de materia prima,
Mayor participación en el Estado	Bases del portal publico inadecuadas
Posicionamiento de marca	Disponibilidad de recursos económicos para marketing

Tabla 4.4: Análisis Proveedores

Interés / requerimiento	Problema percibido
Mantener una relación comercial adecuada y a largo plazo	Calidad del producto, oportunidad de entrega / tiempos de reacción, plazos cortos de pago, burocracia en el proceso de adjudicación,
Estar calificado como proveedor de la empresa	Falta de interés del proveedor de calificarse
Pago oportuno	Procedimientos internos de registro de obligaciones y falta de cumplimiento de documentos habilitantes de pago de acuerdo a políticas establecidas.
Comunicación en el inicio y resultado del proceso de adjudicación	No hay un sistema de comunicación formal, mayor detalle en las especificaciones técnicas
Requerimientos completos: especificaciones técnicas y cantidades	Pedidos adicionales con tiempos distintos de entrega

Tabla 4.5: Análisis Empleados

Interés / requerimiento	Problema percibido
Estabilidad laboral	Tipos de contratos que no aseguran estabilidad
Remuneración competitiva de acuerdo al giro del negocio	Falta de política salarial
Servicios sociales adecuados	Falta de calidad del servicio
Cumplimiento de la normativa legal vigente y aplicable a la empresa	Desconocimiento de descriptivos de cargos, normas reglamentarias, políticas, por problemas en comunicación adecuada.
Cumplimiento de funciones de acuerdo a su contrato laboral	
Capacitación de acuerdo a las necesidades del cargo	
Proceso de inducción adecuado	Falta de interés de las aéreas en la inducción al cargo
Ocupar el cargo de acuerdo al perfil	
Utilización de herramientas para desempeño de funciones	Deficiencia en la provisión de herramientas

Tabla 4.6: Análisis Holding Dine (órgano regulador)

Interés / requerimiento	Problema percibido
Cumplimiento de normativa y políticas corporativas	
Gestión eficiente	Falta de eficiencia en la gestión. No existe un enfoque personalizado a la atención de requerimientos
Imagen de la empresa	Falta de desarrollo de todo su potencial
Empresa con tecnología adecuada	Falta de proyectos inversión y apertura de nuevos mercados
Proyectos de crecimiento empresarial	

Tabla 4.7: Análisis Accionistas (ESTADO)

Interés / requerimiento	Problema percibido
Rentabilidad	Baja rentabilidad
Cumplimiento normativa	N/D
Imagen política	Posibles reacciones laborales

4.2.2.- Estrategia de Negocios

El análisis FODA es una de las herramientas esenciales que provee de los insumos necesarios al proceso de la planeación estratégica, proporcionando la información para evaluar fuerzas, debilidades, oportunidades y riesgos del sector.

El análisis de oportunidades y los riesgos, están relacionados con el estudio de consumidores, competidores y políticas del ambiente externo, como alianzas estratégicas, poder adquisitivo, costos de abastecimiento, etc.

Las fuerzas y debilidades involucran la investigación del mercado doméstico, la carga financiera, productos, mercados, administración, estructura, cultura y recursos financieros de la empresa.

Tabla 4.8: Análisis de Factores Internos por Áreas

FORTALEZAS
COMERCIALIZACIÓN
Gestión ética de procesos de comercialización
Experiencia de vendedores antiguos
Focalización de productos
Mercado cautivo en Fuerza Terrestre
Fidelización de clientes
Amplio portafolio de productos para líneas industrial, institucional y militar
PRODUCCIÓN
Capacidad de producción en alto volumen
Disponibilidad de tecnología de punta en algunas líneas
Disponibilidad de capacidad instalada
Disponibilidad de tecnología de punta en sistemas de información
Posibilidad de crecimiento de planta
CONTROL DE CALIDAD
Laboratorio y disponibilidad de equipos
Control de calidad a proveedores
Control estadístico de procesos
LOGÍSTICA
Conocimiento de los productos y materiales
Conocimiento de los productos y materiales
TALENTO HUMANO
Procesos bien definidos en gestión de Talento Humano
Mano de obra calificada
Cumplimiento de normas y beneficio adicionales
Pago oportuno de sueldos y salarios
ADMINISTRACIÓN
Respeto del orden jerárquico establecido
Manejo ético en la administración de los recursos
Estructura orgánica acorde a las necesidades de la empresa
Conocimiento y coyuntura con principal cliente
DEBILIDADES
COMERCIALIZACIÓN
Falta de perfiles y competencia del personal del área
Cumplimiento parcial del Plan de Comercialización
Falta de herramientas para el personal de ventas
Baja de participación del mercado nacional
Insuficiente personal de vendedores
Falta de comunicación interna entre departamentos
Muchas actividades ajenas en las funciones de los vendedores
Falta de Políticas de Comercialización
Insuficientes Canales de Ventas
Inadecuada distribución de la cartera de clientes

PRODUCCIÓN
Inadecuada planificación
Falta de comunicación interna entre departamentos
Inadecuada determinación de Estándares de Materiales
Inadecuados reportes de Mano de Obra real
Deficiente proceso de diseño
Parte de la maquinaria obsoleta
Falta de Políticas de reposición en maquinaria
Falta de control en horarios extendidos
Deficiente control diario de los Estándares de producción
Falta de fichas técnicas que contengan estándares de calidad
Resistencia del recurso humano para cumplir volúmenes óptimos de producción
Falta Políticas de incentivos y sanciones
CONTROL DE CALIDAD
Falta de fichas técnicas para control de calidad
Falta de cumplimiento de procedimientos internos
Falta de procedimientos que aseguren el control de calidad: Maquila, MP, procesos, producto terminado y pruebas de uso.
LOGÍSTICA
Falta de comunicación interna entre departamentos
Compras
Portafolio limitado de proveedores
Inadecuada planificación de compras
Procedimientos logísticos no responden a las necesidades de la empresa
Incompleta calificación de proveedores
Falta de implementación de procedimientos de compras
Falta de seguimiento en órdenes de compras
Falta de Asesoría Legal permanente
Inventarios
Infraestructura inadecuada
No hay Política de recepción y compra de inventarios
Falta de control para el despacho hacia ventas y producción
Procedimientos mal definidos
Falta de procedimiento de responsabilidades de distribución
Falta de procedimiento de control de inventarios
Débil control de inventarios
A. Fijos
Deficiente información de A. Fijos: Depreciación, custodio, codificación y depreciación.
Falta de procedimientos y políticas para movimiento de activos
TALENTO HUMANO
Falta de Asesoría Legal permanente
Falta de Políticas en Bandas Salariales
Falta de comunicación y coordinación interna entre departamentos

Horas extras no planificadas
Algunos perfiles no se ajusta a necesidades de la empresa
Falta de instrumentos para selección de personal
Falta de disponibilidad de mano de obra: especialidad del trabajo, condiciones legales de contratación
Bajo nivel de Clima Laboral administrativo
GESTIÓN FINANCIERA
Falta de liquidez
Condiciones de préstamos con la matriz
Falta de comunicación y coordinación interna entre departamentos
ADMINISTRACIÓN
Alta rotación de Directivos
Falta de documentación que permita la continuidad de la estrategia de la empresa
Falta de comunicación interna entre departamentos

Tabla 4.9: Análisis Externos por Áreas

OPORTUNIDADES
ECONÓMICO
Creación de políticas para la protección a la Industria Nacional
Política de asignación presupuestaria cuatrimestral en el sector público
POLÍTICO
Fomento al consumo nacional y al sector textil
SOCIAL
Mayor disponibilidad de mano de obra administrativa calificada
TECNOLOGÍA
Disponibilidad y accesibilidad de tecnología de punta
CLIENTE
Potencial de mercado militar total
Amplio mercado industrial
PROVEEDOR
Apertura de alianzas y convenios nacionales e internacionales
Apertura para desarrollar y mejorar productos
COMPETENCIA
Posibilidades de alianzas
Prácticas que posibilitan aprendizaje
HOLDING DINE
Disponibilidad y accesibilidad de tecnología de punta
Disponibilidad y accesibilidad a créditos
Asesoría técnica adecuada en algunas áreas

AMENAZAS
ECONÓMICO
Dificultad en adquirir préstamos a corto plazo (calidad de activos)
Crisis financiera nacional e internacional
POLÍTICO
Impulso al consumo nacional no cumple con estándares de calidad
Incertidumbre por transición al sector público
SOCIAL
Corrupción: Sistema de compras públicas, coimas, fuga de información
TECNOLOGÍA
Posible cambios tecnológicos por transición al sector público
CLIENTE
Posible pérdida de mercado cautivo
Preferencia de precio a calidad
PROVEEDOR
Baja calidad de materia prima
Falta de ética en proveedores puntuales
Plazos de crédito menores
COMPETENCIA
Pérdida de capacidad de acción en el sector privado
Crecimiento de PYMEs
HOLDING DINE
Falta de libertad de acción en algunas áreas: Comercialización, jurídica y tecnología de la información.
Falta de agilidad de respuesta en algunas áreas: Comercialización, jurídica y tecnología de la información.

4.2.2.3.- Visión de FAME

Ser líderes en la confección de vestuario, calzado y equipo de camping, en el mercado militar, industrial e institucional, a nivel nacional, con proyección regional. Socialmente responsables y comprometidos con el desarrollo del país.

4.2.2.4.- Misión de FAME

Producir y comercializar vestuario, calzado y equipo de camping, de uso militar, institucional e industrial, con calidad y precios competitivos, para satisfacer las necesidades de las Fuerzas Armadas y del mercado nacional.

4.2.2.5.- Objetivos de FAME

- Entregar productos competitivos que satisfagan las necesidades de los clientes.
- Captar todo el mercado militar y ampliar la participación en el mercado de terceros en la región.
- Posicionar la marca FAME en los mercados de interés.
- Mantener un eficiente control del inventario y activo fijos.
- Ampliar portafolio de proveedores calificados nacional e internacionales.
- Mantener buenas relaciones con grupos de interés externos.
- Contar con personal calificado.
- Elevar Clima laboral de la empresa.
- Disponer de instalaciones adecuadas y con permisos de los órganos competentes,
- Disponer de tecnología acorde a la línea de negocio.
- Maximizar la rentabilidad.
- Contar con Capital de Trabajo oportuno en condiciones favorables.
- Contar con una Planificación adecuada de la Cadena de Valor.

4.2.2.6.- Valores Institucionales de FAME

- Enfoque hacia el cliente.
- Compromiso y Lealtad institucional.
- Honestidad e integridad.
- Ética empresarial y profesional.

- Iniciativa y creatividad.
- Trabajo en equipo.
- Orientación a resultados.
- Responsabilidad social y ambiental.
- Liderazgo e innovación empresarial.
- Seguridad integral.
- Cumplimiento del Marco Legal

4.2.2.7.- Estrategias de FAME

- Mejorar los estándares de producción de los productos estrellas.
- Cumplir con los tiempos de ciclo de proveedores y producción.
- Mejorar los procedimientos de control de calidad en proveedores, maquila, proceso y producto terminado.
- Mejorar los procesos de diseño de moldería, patronaje, escalado y muestras de los productos, contando con Políticas de Crédito y Descuentos.
- Establecer Canales de Distribución apropiados.
- Establecer convenios con las instituciones militares.
- Gestionar el acercamiento anticipado con las respectivas áreas logísticas de cada fuerza e instituciones públicas y privadas.
- Contar con herramientas de comercialización.
- Implementar el Plan de Comunicación y Publicidad.
- Aplicar el servicio al cliente antes, durante y después de la venta.
- Establecer máximos y mínimos de inventario.

- Establecer Política de recepción, devolución, mantenimiento, ubicación, compra y despacho de inventarios.
- Definir procesos y procedimientos para control de inventarios.
- Definir procesos y procedimientos para control de activos fijos.
- Participar en eventos nacionales e internacionales.
- Utilizar herramientas de búsqueda como internet, base de datos, prensa.
- Cumplir con las normas y leyes vigentes y aplicables a la línea de negocio.
- Cumplir Políticas y Objetivos del órgano regulador.
- Cumplir las leyes laborales.
- Contar con la política de incentivos y sanciones.
- Mantener una comunicación y retroalimentación permanente entre los niveles de la empresa.
- Implementar herramientas de mejora continua.
- Planificar las actividades de la producción.
- Contar con un proyecto de reubicación de la empresa
- Contar con plan de renovación de maquinaria y equipo.
- Mejorar los procesos de Gestión y Control de la empresa.
- Gestionar la suscripción y pago oportuno de los contratos con las Fuerzas Armadas
- Generar Planes de contingencia que ajusten el Plan de Comercialización.
- Optimizar la utilización de la capacidad instalada de la empresa,
- Establecer mínimos de producción.

4.2.3.- Modelo Operativo

En este paso se levantaron los procesos claves, estratégicos y de apoyo de Fabril Fame y que apalanca la producción de la empresa.

4.2.3.1.- Mapa de Procesos

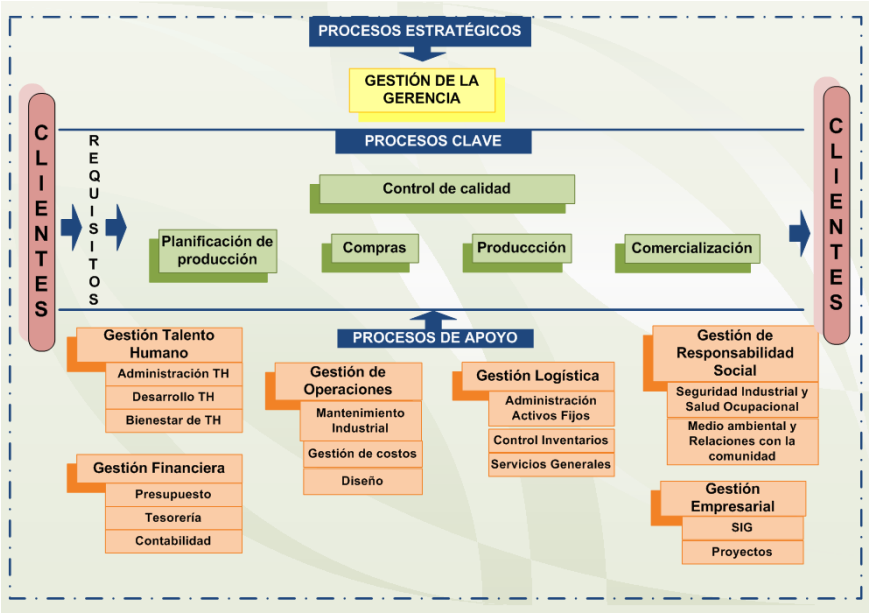


Diagrama 4.3: Mapa de Procesos Fame

4.2.4.- Estructura de la organización

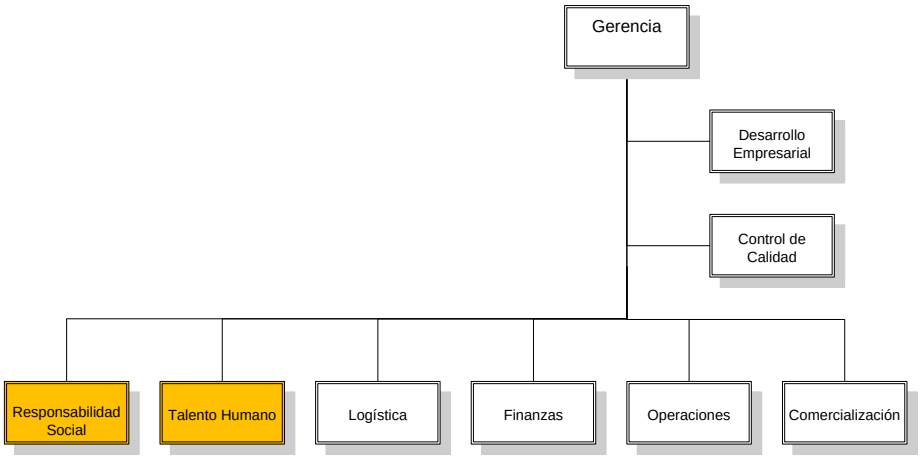


Diagrama 4.4: Estructura Organizacional Fame

4.2.5.- Arquitectura de la información

Proceso Comercialización

Tabla 4.10: Comercialización Planificación de Ventas

RESPONSABLE	ACTIVIDAD
Jefe de Operaciones	Remite el plan de producción de las plantas
Jefe de Comercialización	Analizar cuantitativa y cualitativamente los históricos tanto de plaza, ventas, producto, precio, promoción, estudios de investigación de mercados, informes macroeconómicos, plan de producción y demás variables indispensables, para identificar el o los nichos de mercado a incursionar y el producto a introducir o reforzar
	Elaborar estrategias, planes de acción y metas, para cada objetivo determinado a cumplir en el año lectivo Elaborar la Planificación Operativa anual (**POA)**
	Elaborar el **presupuesto general de ventas** para el año en curso.
	Comunicar a todas las áreas involucradas de la empresa el **POA** mediante presentación, para conseguir la plena coordinación en las actividades comerciales a emprender y que este sea considerado dentro del Plan Operativo Empresarial.
	Solicitar apoyo y asesoramiento tanto de la Gerencia General como con el Holding Dine, para obtener recurso económicos, humanos y demás herramientas de trabajo
	Bajar o transmitir toda la información del plan Operativo anual comercial POA al equipo de trabajo comercialización (Vendedores, asistentes, especialistas, etc), para emprender rápidamente en las nuevas actividades o funciones asignadas.
Especialista Fuerza Terrestre / Terceros	Ejecutar las estrategias y planes de acción encomendadas por la Jefatura Comercial de acuerdo a los cronograma previsto en el POA
	Asignar el **presupuesto general de ventas** a las diferentes regiones del país, vendedores, clientes actuales y nuevos.
	Planificar con cada vendedor las acciones a cumplir de acuerdo a cada estrategia u objetivo planteado por la jefatura comercial, según **POA**.

Asesor Comercial	Ejecutar las estrategias y planes de acción encomendadas por el Especialista en Ventas según el POA **cronograma de trabajo.**
	Presentar o comunicar el presupuesto general de ventas de los diferentes clientes actuales y nuevos, vía mail y personalmente al Jefe de Comercialización.
	Seguimiento constante al cliente, para hacer cumplir el presupuesto asignado.

Tabla 4.11: Comercialización Facturación con Vendedor

RESPONSABLE	ACTIVIDAD
Técnico en Facturación	Recepción de documentos de Respaldo • Cotización emitida al cliente por parte del asesor comercial. • Documento de compra emitido por el cliente (orden de compra, contrato, cotización aprobada, solicitud vía mail, oficio). • Acta de entrega y recepción con sus respectivas firmas.
	Ingresar información al sistema e imprimir factura.
	Generar las órdenes de venta de las cuales inician el proceso hasta finalizar en la facturación
	Impresión de Factura
	Legalizar las facturas con firmas de: facturado por, Vendedor, jefe de comercialización y recibí conforme del cliente.
	Entregar Factura al Vendedor para la firma de recibí conforme del cliente.
Asesor Comercial	• Entrega de factura al cliente para legalización de firma de recibí conforme en el caso de que el cliente se encuentre dentro de la provincia. • Envío (transporte, correo, vía fax) de factura original al cliente para la legalización de firma de recibí conforme en el caso de que el cliente se encuentre fuera de la provincia.
	• Recopilar copias de factura con la firma de recibí conforme. • Se entrega las facturas: Original al cliente, copia 1 para ventas, copia 2 para finanzas, copia 3 y 4 bodega calzado y vestuario.

Tabla 4.12: Comercialización Facturación Puntos de Venta

RESPONSABLE	ACTIVIDAD
Persona responsable del punto de venta	Atender los requerimientos y pedidos de los clientes
	Emitir órdenes de venta y factura al cliente.
	Realizar el cobro si es en efectivo o registrar para descuento en el caso de empleados de Fabril Fame
Técnico en Facturación	Recopilar documentos de respaldo. Notas de Venta Facturas Reporte de Venta Depósitos
	Ingresar al Sistema órdenes de venta o facturas en forma individual, para descargo de inventario, de aquellos puntos que no estarán en red.
	Imprimir la Factura o nota de venta
	Verificar la nota de venta o factura con reporte de venta y depósitos.
	Elaborar cuadros de ventas diarios registrando el número de depósito y nota de venta.
	Entregar facturas y notas de venta a Contabilidad con documentos de respaldo para que se registren los pagos y depósitos dentro del sistema.
	Entregar la copia de Factura o nota de venta a cada punto de venta o responsable del mismo para verificación de datos.
	Cuando se trata de facturas o notas de venta emitidas a crédito a empleados se realiza el mismo procedimiento a excepción del registro de depósitos. En este caso se envía un listado con los valores a descontar del personal al Departamento de Recursos Humanos.

Tabla 4.13: Comercialización Facturación Muestras, Ropa de Trabajo y Publicidad

RESPONSABLE	ACTIVIDAD
Técnico en Facturación	Recepción de documentos de Respaldo Oficio de solicitud emitido por el cliente. (En caso de ser ropa de trabajo el documento emitido por el jefe de Recursos Humanos). Formato de muestras no retornables, debidamente legalizado con firmas de solicitante, autorizado,

	responsable, entregué conforme y recibí conforme. Guías de Transferencia legalizadas
	Ingresar información al sistema e imprimir factura y legalizarla
	Impresión de Factura
	Legalizar factura con firmas de facturado por, Vendedor, Jefe de Comercialización.
	Envío de factura con documentos de respaldo a Contabilidad para su registro.

Tabla 4.14 Comercialización Facturación Manual

RESPONSABLE	ACTIVIDAD
Asesor comercial	Recepción de oficio solicitando factura manual por parte del cliente.
	Envío al departamento Financiero de oficio emitido por el cliente, oficio del jefe de comercialización y cuadro de posibles fechas de entrega de producto al cliente.
Técnico en facturación	Recepción de documentos de Respaldo con las firmas de autorización del Gerente General y Jefe Financiero. Cotización emitida al cliente por parte del Asesor Comercial. Documento de compra emitido por el cliente (orden de compra, contrato, cotización aprobada, solicitud vía mail, oficio).
	Generar factura manual desde el sistema Baan
	Impresión de Factura
	Legalización de facturas con firmas de: facturado por, Vendedor, jefe de comercialización.
	Entrega de Factura al Vendedor para la firma de recibí conforme del cliente.
Asesor comercial	• Entrega de factura al cliente para legalización de firma de recibí conforme en el caso de que el cliente se encuentre dentro de la provincia. • Envío (transporte, correo, vía fax) de factura original al cliente para la legalización de firma de recibí conforme en el caso de que el cliente se encuentre fuera de la provincia. Recuperación de copias de factura con la firma de recibí conforme. Original al cliente, copia 1 para ventas, copia 2 para finanzas, copia 3 y 4 bodega calzado y vestuario.

Técnico de facturación	Entrega a auxiliar contable de copia de factura y documentos de respaldo.
	Seguir con el proceso de la orden de venta generada para fabricar las prendas que constan en la factura manual
Vendedor / técnico de facturación	Conciliación de información con Bodegas y área contable de entregas parciales o totales del producto. (despachos de los artículos ya fabricados)
Técnico de facturación	Generar retro-ordenes en caso que las entregas sean parciales y que se deberán liquidar en su totalidad objeto de la factura manual, en coordinación con inventarios y cartera.

Tabla 4.15 Comercialización Facturación Varios

RESPONSABLE	ACTIVIDAD
Responsable de la venta	Entrega documento a comercialización para factura de varios indicando los ítems a facturar precios y más datos.
Técnico de facturación	Generar factura manual desde el sistema Baan
	Impresión de Factura
	Legalización de facturas con firmas de: facturado por, responsable de la venta, jefe de comercialización.
	Entrega de Factura al responsable de la venta para la firma de recibí conforme del cliente.
	Entrega a auxiliar contable de copia de factura y documentos de respaldo.

Tabla 4.16 Comercialización Facturación Consignación

RESPONSABLE	ACTIVIDAD
Asesor comercial	Recepción de documentos de Respaldo • Convenio de venta entre la Empresa y el Cliente. Documento de pedido emitido por el cliente
Técnico de facturación	Generar Orden de venta en el sistema para despacho de mercadería(Reaprovisionamiento-consignación)
Especialista de bodegas	Despacha mercadería, imprime guía de remisión
Conductor	Transporta mercancía al cliente con guía de remisión.
Asesor comercial	Legaliza las entregas.
	Entrega a Facturación, de documentos con liquidaciones y reportes de los artículos vendidos por el cliente para factúralos.

Técnico de facturación	Generar orden de venta para facturar los artículos indicados en las liquidaciones y reportes que entrega en Vendedor.
Asesor comercial	Reingreso a Bodega de los artículos que no fueron vendidos por el cliente a consignación
Técnico de facturación	Genera Orden de venta de devolución (reingreso a bodega) de mercancía a consignación no vendida.
Especialista de bodegas	Decepcionar la mercadería

Tabla 4.17 Comercialización Cierre Mensual Facturación

RESPONSABLE	ACTIVIDAD
Técnico de facturación	Ingreso al sistema hasta el 31 de cada mes.
	Envío de documentación al Departamento Financiero (Facturas, Notas de venta, depósitos, notas de crédito).
	Revisión de documentos Reporte de documentos no actualizados con el área contable.
	Emisión del Reporte del diario de ventas.
	Cuadre de ventas en coordinación con: Cartera, Inventarios, Especialista de Ventas a Terceros (formato **reporte de ventas**)
	Elaboración de **cuadro de ventas totales** y por vendedor.
	Elaboración de cuadro de **cumplimiento de presupuesto de ventas** por vendedor.
	Archivar Documentación
	Envío de copias de documentación con respaldos a departamento financiero, puntos de venta y bodegas.
	Elaboración y envío al departamento financiero de reportes de documentos anulados (Facturas, notas de venta, notas de crédito)

Tabla 4.18 Comercialización Emisión Notas de Crédito

RESPONSABLE	ACTIVIDAD
Asesor comercial	Recepción de oficio de solicitud de emisión de nota de crédito por parte del cliente, adjuntando la copia original de la factura a ser anulada.
	Elaboración de oficio firmado por el jefe de comercialización solicitando al Departamento

	Financiero la emisión de la nota de crédito adjuntando el oficio del cliente y factura original.
Técnico en facturación	Recepción de documentos de Respaldo con las firmas de autorización del Jefe Financiero.
	Nota de crédito a la factura sea esta por devolución o cambio de factura. (En caso de ser devolución se adjunta el acta de entrega y recepción firmada por el responsable de la bodega que recibió el producto)
	Impresión de la Nota de crédito.
	Generar una nueva orden de venta en caso de que se necesite reposición de prendas con falla de fábrica, objeto de la venta.
	Generar nueva orden de venta cuando se trate de notas de crédito por cambio de factura.
	Legalización de facturas y nota de crédito con firmas de: facturado por, asesor comercial, jefe de comercialización.
	Entrega de Factura y Nota de crédito al Asesor Comercial para la firma de recibí conforme del cliente.
Asesor comercial	• Entrega de factura y nota de crédito al cliente para legalización de firma de recibí conforme en el caso de que el cliente se encuentre dentro de la provincia. • Envío (transporte, correo, vía fax) de factura y nota de crédito al cliente para la legalización de firma de recibí conforme en el caso de que el cliente se encuentre fuera de la provincia. Recuperación de copias de factura y nota de crédito con la firma de recibí conforme. Original al cliente, copia 1 para ventas, copia 2 para finanzas, copia 3 y 4 bodega calzado y vestuario.
Técnico en facturación	Envío de documentación de respaldo al Departamento Financiero con nota de crédito y factura anulada y nueva factura para el registro en el área contable.

Tabla: 4.19 Comercialización Ventas

RESPONSABLE	ACTIVIDAD
Cliente	Realiza el pedido con las especificaciones requeridas, al asesor comercial ya sea vía mail, fax, orden de compra, oficio, documento de adjudicación o proforma aprobada.

Asesor comercial	Elabora el documento en Excel del pedido del cliente (prenda nueva) con las especificaciones técnicas, modelo y cantidad, y pasa a planificación y costos para que indique el tiempo de entregas y costo de la prenda, para envió de cotización al cliente.
	Elabora la cotización dentro del sistema pasa a Especialistas o Especialistas de ventas, para la revisión y aprobación, y envía al cliente.
	Confirma dentro del sistema la aceptación de la cotización del cliente e informa a la Jefatura Comercial o Especialistas y adjunta formato con las especificaciones y demás datos del producto solicitado por el cliente.
Especialista FFTT o Especialista de Terceros	Procesan la oferta en orden de venta, o a su vez generan directamente la orden de venta, ingresando dentro del sistema, especificaciones técnicas, modelos, cantidades y tallas.
	Una vez generada la orden por el especialista de ventas el Jefe de Comercialización firma la orden.
Asesor comercial	La orden de venta es entregada a Operaciones para iniciar el procedimiento de producción.
	Da seguimiento de la producción vía telefónica, visual.
Especialista de Bodegas	Debe comunicar que el producto se encuentra listo en bodega para proceder con las entregas, realiza el procedimiento correspondiente imprime la guía entrega al conductor.
Asesor comercial	Entrega el producto al cliente, hace firmar la factura, actas de recepción entrega, guía de remisión.
Especialista de Bodegas	Entregar al asesor comercial las copias de factura, actas de entrega recepción, guías de remisión
Asesor comercial	Realiza el seguimiento de cobro y retiro de retenciones.

Tabla 4.20 Comercialización Licitaciones

RESPONSABLE	ACTIVIDAD
Asistente de Comercialización	Buscar licitaciones en compras públicas, para participación de la empresa en la oferta de productos.
	Definir las invitaciones a licitar.
	Entregar la invitación al Especialista que corresponde.
Especialista FFTT o	Designar al vendedor sus licitaciones

Especialista de Terceros	correspondientes para que inicien el proceso. En el caso de la Fuerza Terrestre el especialista inicia el proceso de licitación.
Asesor Comercial	Elabora la licitación en coordinación con Operaciones y Compras.
	Entrega de la licitación en la fecha dispuesta en las bases.
	En caso de ser adjudicado se procede a firmar el contrato, convenio o documento de adjudicación y luego se procede con la recepción del anticipo. Si esta no es adjudicada se cierra el proceso de licitaciones.
	Elaborar órdenes de venta con especificaciones que se encuentran en la licitación.
	Realizar seguimiento de la producción y entrega del pedido
Especialista de Bodegas	Debe comunicar que el producto se encuentra listo en bodega para proceder con las entregas, realiza el procedimiento correspondiente imprime la guía entrega al conductor.
Asesor Comercial	Entrega el producto al cliente, hace firmar la factura, actas de recepción entrega, guía de remisión.
	Entregar al Asesor Comercial las copias de factura, actas de entrega recepción, guías de remisión
	Realizar el seguimiento de cobro y retiro de retenciones

Tabla 4.21 Comercialización Creación de Crédito a Clientes

RESPONSABLE	ACTIVIDAD
Jefe de Comercialización	Enviar la carta de presentación al cliente, indicando las características del producto, tipos de embalaje, precios, dirección de la empresa.
	Solicitar al cliente documentos certificados de la empresa: Cédula de identidad, Nº de pasaporte de representante legal, RUC, direcciones, contactos, referencias bancarias nacionales.
	Realiza la verificación en el SRI y referencias bancarias nacionales.
	Comunicar al cliente las condiciones y políticas de crédito. (30 días máximo).
	Entregar al Jefe financiero la documentación del cliente para aprobación del crédito de acuerdo a las **políticas de crédito.**

	Si el cliente no es aprobado se cerraría el proceso de apertura de crédito
	Enviar la carta de presentación al cliente, indicando las características del producto, tipos de embalaje, precios, dirección de la empresa.
Jefe Financiero	Si es aprobado registrar al cliente en el sistema.
Jefe Comercialización	Archivar documentación legal de todos los clientes.

Tabla 4.22 Comercialización Cobro a Clientes

RESPONSABLE	ACTIVIDAD
Jefe de Comercialización	Realizar seguimiento verificando la fecha de vencimiento de las facturas de los clientes según las **cuentas por cobrar**
Asesor Comercial	Contactar con el cliente y coordinar el pago ya sea mediante cheques o transferencias.
	Coordinar con el tesorero la efectivización de transferencias en el banco.
	Retirar los cheques los días establecidos por el cliente para su pago.
	Conciliar el valor recibido con las facturas pagadas.
	Entregar al Tesorero el cheque con su respectivo recibo de caja.
Tesorero	Depositar en el banco y realizar el respectivo ingreso de caja. Entregar a contabilidad los comprobantes

Tabla 4.23 Comercialización Promoción y Publicidad

RESPONSABLE	ACTIVIDAD
Jefe de Comercialización	Elaborar el plan de marketing considerando medios y formas de publicidad.
	Coordinar con Marketing de la matriz HD.
Asistente de Comercialización	Segmentar los ítems de publicidad y divide los montos a gastarse para cada ítem de forma mensual.
Jefe de comercialización	Elabora el **presupuesto de marketing** tomando como referencia del 0.5 al 1% de la totalidad de las ventas presupuestadas en el año.
	Envío del Presupuesto de Marketing al Jefe Financiero para su aprobación
Jefe Financiero	Envía el presupuesto aprobado al Jefe de Comercialización
Jefe de	Revisar Plan de Marketing aprobado por el

Comercialización	Departamento Financiero
	Enviar Plan de Marketing a Gerencia para su aprobación.
Gerente	Analiza plan. Si: Envía para implementación. No: Enviar para ajuste
Departamento de Comercialización	Ejecución del Plan de Marketing
Asistente de Comercialización	Solicitar a Marketing de Holding Dine, apoyo en la ejecución de actividades promociónales y comunicacionales que necesite comercialización. (Relanzamientos, vallas publicitarias, comunicación en medios directos).

Tabla 4.24 Comercialización Satisfacción de Clientes

RESPONSABLE	ACTIVIDAD
Aseso Comercial	Realizar la encuesta de satisfacción al cliente una vez cerrada la venta, mediante formato establecido para este fin.
Asistente de Comercialización	Consolidar y tabular las encuestas, formato de tabulación de encuestas. Elaborar Informe.
	Se ingresan los resultados obtenidos al BSC semestralmente.
Especialista de Terceros y Especialista de FFTT.	Realizar seguimiento a visitas de vendedores directamente con el cliente.
Asistente de Comercialización	Receptar percepción de clientes en cuando a productos y servicios. Al encontrar una NO conformidad, enviar a Desarrollo Organizacional para su respectivo análisis y seguimiento.
Especialista de FFTT. Especialista de Terceros y Jefe de Comercialización	Analizar resultados y toma de acciones preventivas, correctiva y/o mejora
Jefe de Comercialización	Se envía a Marketing de Holding dine y Jefes de la organización.

Proceso Producción

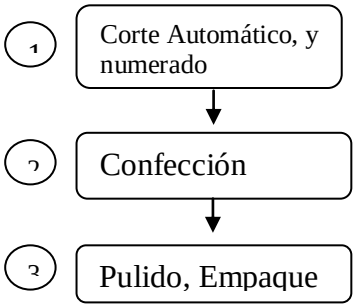


Diagrama 4.5: Proceso Comercialización

Tabla 4.25: Producción

RESPONSABLE	ACTIVIDAD
Jefe de Operaciones	Recibe la Orden de Venta (en el sistema Baan) de Comercialización.
	En el caso de pedido autorizados por la Gerencia General, recibir en el formato Orden de Venta Física fuera del sistema Bann
	Realizar la planificación de operaciones en el sistema Baan de acuerdo al **Procedimiento de Planificación de la Producción.**
Analista de Producción	Genera la Orden de Producción en el sistema Baan.
	Se crea la Orden de Compra en el sistema Baan y se procede de acuerdo al Proceso de Adquisiciones.
Técnico de Bodegas	Ingresar el material a Bodega de acuerdo al procedimiento de Recepción y Almacenamiento de Materia Prima y Producto Terminado.
Jefe de Operaciones	Se crea el Requerimiento de Materiales a bodegas en el sistema Baan para posteriormente el operario (líder) retire los insumo y/o materiales.
Jefe de Producción	Entrega la Orden de Producción a Control de Calidad, Logística y operario (líder de línea).

Tabla 4.26: Producción Corte

RESPONSABLE	ACTIVIDAD
Obrero (Líder de corte)	Retira materiales de bodega de materia prima según Orden de Producción.

Tabla 4.27: Producción Corte Automático

RESPONSABLE	ACTIVIDAD
Especialista de Diseño	Entrega estándar según tallas a cortar para tendido de tela y entretelas.
Obrero de corte	Realiza el tendido de tela y entretelas de acuerdo a la Orden de Producción.
	Realiza el Corte automático según especificaciones técnicas, entregadas por el Especialista de Diseño, en máquina de Cortadora Gerber. (Instructivo FF-MIINS-003)
	Trasladar los cortes en los coches a la sección de numerado
	Numerar piezas con máquina numeradora, con el código de acuerdo al corte realizado (Número de día, talla y consecutivo)
Operario (línea de confección)	Recibe y traslada los materiales cortados y numerados a la línea de confección.
Obrero de corte	Se almacena el material residual de tela en los coches para ser manejados tratados de acuerdo al Procedimiento de Manejo de Desechos Sólidos.

Tabla 4.28: Corte Manual

RESPONSABLE	ACTIVIDAD
Especialista de Diseño	Entrega de moldes al Obrero de corte.
Obrero de corte	Tender la tela y entretela en la mesa de trabajo por unidad traje formal.
	Colocar moldes en la tela y entretela a cortar.
	Dibujar trazos de acuerdo a las tallas en la Orden de Producción
	Efectuar corte manual.
	Numerar manualmente las piezas cortadas de acuerdo a la codificación (Número de día, talla y consecutivo) para su posterior traslado a la sección de fusionado.
	Fusionar tela y entre tela.
	Se almacena el material residual de tela en los coches para ser tratados de acuerdo al Procedimiento de Manejo de Desechos Sólidos.

Tabla 4.29: Producción Confección

RESPONSABLE	ACTIVIDAD
Operario	Retira de la sección corte las piezas cortadas y numeradas para el proceso de producción.
	Ensamble de piezas de acuerdo a Instructivo de Vestuario FF-PRIN-001
	Registra producción diária en el formato Registro de Horas y cantidades y entrega diariamente al Especialista de producción de vestuário.

Auxiliar de Control de Calidad	Ejecutar el Proceso de Control de Calidad de Producto en Proceso.
Operario	Entrega a la sección de pulido y empaque el producto.
Auxiliar de Control de Calidad	Ejecutar el Proceso de Control de Calidad de Producto Terminado.

Tabla 4.30: Producción Pulido y Empaque

RESPONSABLE	ACTIVIDAD
Obrero de sección de pulido y empaque	Realiza la última revisión de costuras y pulido (corte de hilos).
	Colocar en una funda el producto terminado de acuerdo a la numeración y talla.
	Solicitar al Asistente de Producción la Guía de Fabricación, (En el sistema Bann debe estar ingresado los tiempos de fabricación y constar en número de orden a terminar), para que inicie el Procedimiento de Ingreso a Bodega.

Tabla 4.31: Producción Calzado

RESPONSABLE	ACTIVIDAD
Vendedor	Entrega el pedido de elaboración indicando el tipo, talla, cantidad, fecha de recepción y fecha de entrega de producto detallado en el registro Orden de Trabajo.
Jefe de Operaciones	Analiza el pedido y establece la fecha de entrega de pedido de acuerdo al **Procedimiento de Planificación de la Producción.** En el caso de no poder entregar en la fecha solicitada por el cliente, el vendedor re-negociara la

	fecha con el cliente.
	Solicitar a Bodega verificar la existencia de materiales.
Técnico en Bodega	Solicitar a Logística la **Solicitud de Compra**, de acuerdo al pedido de materiales para la Orden de Trabajo de acuerdo a **Lista de Materiales**
Especialista de Adquisiciones	Recepta pedido y procede a la adquisición de insumos.
Técnicos en Bodega	Recepta los insumos, notifica a Producción y Control de Calidad de Materia Prima para los análisis correspondientes.
Auxiliar de Control de Calidad (laboratorio)	Efectúa los análisis correspondientes de acuerdo a los procesos de Control de Calidad.
	Si los materiales no son aceptados se procede a la devolución caso contrario ingresan los insumos para la producción
Especialista en Producción de Calzado	Emite: **Guía de Fabricación** registrando número de Orden de Producción, tipo de calzado, fecha, cantidad, talla y firmas de responsabilidad. **Pedido a Bodega** donde se registra el pedido de materia prima de acuerdo a la orden de fabricación generadas en el sistema Bann.
Líder de cada sección	Retira insumos que le corresponden.
	Entrega a Operadores de cada sección los insumos
Operarios	Empieza las actividades de producción de acuerdo al **INSTRUCTIVO DE TRABAJO DE CALZADO**.
	Terminado el proceso productivo se entrega a Bodega de Producto terminado para despacho a cliente

Tabla 4.32: Producción Seguimiento del Proceso

RESPONSABLE	ACTIVIDAD
Especialista en Producción de Calzado	Diariamente se efectúa ingreso de órdenes de producción en el sistema Bann. Anunciar diariamente Operaciones y Ordenes Terminadas en el sistema Bann

Especialista en Producción de Calzado	Efectúa un seguimiento y control de la producción y toma las acciones correspondientes en el caso de no ir cumplimiento lo planificado. Reporta a Operaciones para el seguimiento correspondiente.
Especialista en Producción de Calzado	Mensualmente obtener los Índices de Producción, ingresa en el sistema Balance Scorecard y reporta Informe de Producción a Desarrollo Empresarial y Gerencia General.
Especialista de Sistemas Integrados de Gestión	Analizar y efectúa un seguimiento de los Indicadores de Gestión reportados. Empatar con los procesos de Gestión de la Calidad.

Tabla 4.33: Producción Diseño

RESPONSABLE	ACTIVIDAD
Especialista de Diseño	Entregar Cuadro de Tallas y Especificaciones de Confección al Jefe de Control de Calidad.
Jefe de Control de Calidad	Elabora las Bases Técnicas.
Auxiliar de Control de Calidad en PP y PT.	Realizar las inspecciones de las muestras y de los Set de Tallas en cuanto a variables de confección y variables de materiales. Verificando las especificaciones del producto el cual se registra en el formato Reporte de Auditoria de Calidad.
Auxiliar de Control de Calidad PP y PT	Revisar la calidad visual y dimensional de la prenda empleando la especificación de confección y el cuadro de medida, respectivamente, entregados por el Especialista de Diseño.
	Si el producto no cumple con especificaciones, reprocesar hasta obtener la conformidad de la prenda. Y enviar al Jefe de Control de Calidad.
Jefe de Control de Calidad	Aprobar la Especificación y Cuadro de Medidas.

Tabla 4.34: Logística Adquisiciones

RESPONSABLE	ACTIVIDAD
Especialistas de Producción y/o Especialista de Mantenimiento Industrial	Elaborar la Solicitud de Compra en el sistema ERP Baan, según necesidades y/o planificación.
Especialista en Adquisiciones	Aprobar en el Baan las solicitudes de compra de hasta USD 3.000,00 entrantes
Jefe de Logística	Aprobar en el Baan las solitudes de hasta USD 10.000,00.
Gerente General	Aprobar en el Baan las solicitudes de hasta USD 100.000,00.
Holding Dine	Aprobar las solicitudes de más de USD 100.000,00.

Especialista de Adquisiciones	Disponer de acuerdo al artículo a adquirir la búsqueda de proveedores calificados
Especialista o Técnicos en Adquisiciones	Definidos los proveedores calificados, atarlos a la solitud de compra para convertirlos en solicitud de oferta (Baan).
Técnicos de Adquisiciones	Elaborar el cuadro de comparativo de ofertas y entregar al Especialista de Adquisiciones para su revisión.
Especialista de Adquisiciones	Presentar el cuadro comparativo con las propuestas respectivas para la aprobación del Jefe de Logística y Gerencia. Hasta USD 10.000,00
	Si el monto supera los USD 10.000,00 entregar la información, en el formato cuadro de requerimientos, con los proveedores calificados sugeridos al Jefe de Logística para el proceso de licitación
Jefe de Logística	Si el monto está entre los USD 10.000,00 hasta USD 100.000,00 se convoca a procedimiento de licitación interno. Si el monto supera los USD 100.000,00 notificar a Gerencia para que el proceso lo realice Holding Dine. En ambos casos se convoca únicamente a proveedores calificados.
Jefe de Logística	Notifica la resolución al Especialista de Adquisiciones vía correo electrónico u oficio.
Especialista o Técnicos en Adquisiciones	Ingresar las ofertas de proveedores en el sistema BaaN.
Especialista o Técnicos en Adquisiciones	Convertir en el BaaN la oferta ganadora en Orden de Compra y notificar al proveedor, siempre con los documentos de respaldo respectivos.
Técnicos en Adquisiciones	Si es una orden de compra de materia prima, producto terminado o repuestos lanzar la Orden de Compra a Bodegas (Warehousing).
	Si es una orden de compra de servicios, realizar el proceso de recepción de servicios en el módulo de compras, cuando haya llegado la factura aprobada por el área correspondiente. En temas de servicios ambientales coordinar directamente con el departamento de responsabilidad social
Técnicos en Bodegas	Realizan el proceso de recepción de materiales de acuerdo al respectivo procedimiento con ubicaciones en coordinación con el departamento de adquisiciones y colocando el número de orden de compra en la factura e imprimiendo la recepción de bodega para pasar estos documentos a los técnicos de adquisiciones.
Técnico de Bodegas	Solicita la aprobación de la factura a Control de

	Calidad mediante un sello en la misma y la entrega al Dpto. de Adquisiciones.
Especialista / Técnicos de Adquisiciones	En caso de rechazo del material, se realiza una orden de compra de devolución y se procede a la devolución de acuerdo al procedimiento respectivo.
Técnicos en Adquisiciones	Realizar el proceso de cierre de compras.
Técnicos de Adquisiciones	Entregar factura aprobada, orden de compra autorizada y recepción de bodega al Departamento Financiero para el pago correspondiente.

Tabla 4.35: Logística Evaluación del Desempeño

RESPONSABLE	ACTIVIDAD
Especialista en Adquisiciones	Realizar la evaluación de forma anual a todos los proveedores calificados, utilizando el formato **"**Evaluación del desempeño de proveedores**"**
	La evaluación se la realizará en coordinación con la Jefatura de Responsabilidad Social y Jefatura de Control de Calidad.
	Comunicar los resultados de la evaluación (vía fax o mail) a los proveedores calificados por separado y en el caso de requerirse pedir planes de acción.
	En caso de que un proveedor haya sido calificado como proveedor tipo D este pondrá calificarse como proveedor nuevo de acuerdo al procedimiento de calificación de proveedores en una nueva convocatoria.

Tabla 4.36: Logística Calificación de Proveedores

RESPONSABLE	ACTIVIDAD
Especialista de compras	Invitación a proveedores en general de acuerdo a los grupo establecidos por la organización a calificarse y recalificarse, por los medios que se considere oportuno (prensa, correo electrónico, fax o comunicación de la empresa).
Técnicos de Adquisiciones	Recepción de carpetas con los documentos habilitantes.

Técnicos de Adquisiciones	Llenar el formato Identificación de proveedores de bienes y servicios
Especialista de adquisiciones	Proceder a solicitar, cuando las circunstancias lo permitan, muestras de los productos ofertados, además de planificar una visita de carácter técnico con el Dpto. de Control de Calidad y Responsabilidad Social (Ambiente y Seguridad).
Especialista de adquisiciones	Cuando existan proveedores que no han entregado documentación relevante, notificar a los mismos que este hecho se considerará un demérito en la evaluación del desempeño de proveedores, hasta que se cumplan los requisitos establecidos y eso se notificará de acuerdo al procedimiento.
Especialista de adquisiciones	Proceder a la calificación de los proveedores de la organización, los proveedores de servicios ambientales serán coordinados con el departamento de responsabilidad social
Técnicos de adquisiciones	Notificar a cada uno de los proveedores sobre si fueron o no calificados por la organización y su respectivo justificativo, por los medios que se considere oportuno (prensa, correo electrónico, fax o comunicación de la empresa) para que el proveedores tome las acciones del caso.

Tabla 4.37: Control de Calidad Materia Prima

RESPONSABLE	ACTIVIDAD
Técnico bodega de materia prima	Comunicar al personal de Control de Calidad mediante correo electrónico o verbalmente la llegada de materia prima, junto al Reporte de Materia Prima y enviar al Esp. de Control de Calidad, Jefe de Operaciones, Esp. de Bodegas, Esp. de Compras y Jefe de Comercialización.
Esp. De control de calidad de MP	Realiza la aplicación de análisis y/o pruebas correspondientes para aceptación o rechazo, de acuerdo a los procedimientos del manual de Laboratorio MP.
Auxiliar de laboratorio de MP	Tomar la muestra física de mediante tablas AQL.
	Identificar el producto en cuarentena hasta realizar los análisis, colocando stikers amarillos.
	Realizar análisis según especificaciones técnicas ya sea físico, químico o comparativo mediante el Manual de laboratorio de MP en donde constan los instructivos,

	métodos, manuales, normas utilizados para este fin.
	Emitir el Informe de Análisis físico-químico y enviar al Especialista de control de calidad de materia prima para que valore y analice el informe del material.
Especialista de control de calidad materia prima	Comparar con las normas INEN, Normas Internacionales, especificaciones y toma la decisión de aprobar o rechazar el material. En casos especiales cuando no cumpla el material las especificaciones pero el cliente acepta en esas condiciones, deberá ser aprobado por el mismo y registrado en el formato Registro de producto no conforme.
El auxiliar de laboratorio MP	Colocar el sello de aprobación o rechazo, en el producto. El verde es aprobado, el rojo es rechazado y amarillo en cuarentena.
	Elabora el Reporte de control de calidad de materias primas aprobadas y envía al Jefe de Control de Calidad, Jefe de Operaciones, Especialista de Producción, Jefe de Logística, Especialista de Adquisiciones y Especialista de Control de calidad de MP.
Especialista de control calidad de materia prima	Si se rechaza el material analizado, generar el registro de producto no conforme y enviar a Sistema de Gestión de Calidad para verificar las acciones tomadas para solucionar la no conformidad y no se vuelva a presentar.
El Técnico de bodega de materia prima	Coloca el material rechazado por Control de Calidad en el área asignada para producto no conforme.
Auxiliar de control de calidad de MP	Identificar productos no conformes con sticker rojos.
Especialista de Adquisiciones	Realiza la gestión para la devolución al proveedor. **NOTA:** no deberá permanecer en la bodega por mucho tiempo máximo 48 horas.
Jefe de Logística	Convocar a comité de la empresa mensualmente para determinar la disposición final del producto no conforme en el caso de que el proveedor no retire el material.
Comité	Notifica la disposición final del producto al Especialista de Bodega e informa al Gerente General.

Tabla 4.38: Control de Calidad en Proceso y Productos Terminados

RESPONSABLE	ACTIVIDAD
Especialista de control de calidad en proceso y producto terminado	Receptar una copia de la Orden de Trabajo en la cual constan todas las especificaciones del cliente y la Programación de Producción.
	Elaborar la Planificación de Control Calidad de Producto en Proceso y Terminado y difunde a los Auxiliar de Control de Calidad PP y PT.
Auxiliar de Control de Calidad PP y PT.	Realiza el control de calidad en proceso y terminado, de acuerdo a la planificación dependiendo del producto, en cada etapa del proceso (corte, confección, acabados) verificando las especificaciones del producto el cual se registra en el formato Auditoria de Calidad (Terminado) y Hoja Volante (Proceso). Y enviar resultados al Especialista de PT y PP Nota: Para productos realizados a la medida se debe verificar las medidas tomadas del cliente al 100% y las especificaciones del cliente, mediante muestreo AQL
Especialista de control de calidad en proceso y producto terminado	Si el producto no cumple con especificaciones, se registra en el formato de No Conformidad el cual se envía al SGC para su direccionamiento al Jefe de Operaciones y efectúe la corrección, el plan de acción y verifique su cumplimiento.
Auxiliar de Control de Calidad PP y PT.	Comunica al Líder de línea verbalmente que el producto no cumple con las especificaciones para suspender provisionalmente la confección de las prendas defectuosas.
Jefe de Operaciones	Si el producto no conforme tiene posibilidad de arreglo se decide regresar a reproceso y es registrado en el Registro de producto en reproceso.
Auxiliar de Control de Calidad PP y PT.	Realiza nuevamente el ciclo de revisión de control de calidad en el reproceso de productos y sobre el producto terminado.

Tabla 4.39: Control de calidad en Productos Tercerizados

RESPONSABLE	ACTIVIDAD
Especialistas de control de calidad PT y PP	Recepta Requerimiento de Especificaciones técnicas del producto por adquirir.
Especialistas de control de calidad PT	Genera el formato Auditoria de Calidad y Auditoria de Medidas en donde constan las especificaciones y entrega al Auxiliar de Control de Calidad PP y PT.
Auxiliar de Control de	Realizar inspección de producto en la bodega de PT de

Calidad PP y PT.	acuerdo al formato Auditoria de Calidad, colocar el sticker respectivo (verde aprobado y rojo rechazado) y envía resultados al Especialista de control de calidad PP y PT.
Especialista de control de calidad PP y PT	Si no cumple la especificación emite un informe a Jefe de Logística para que tomar las acciones necesarias y es registrado en el formato Registro de producto no conforme.
	Si el producto se aprueba, comunicar, vía mail, al Especialista en Administración de Bodegas y al Especialista de Adquisiciones. Y se coloca el sello de aprobación en la factura del proveedor.

Tabla 4.40: Control de Calidad en el Proceso de Muestras de Materia Prima

RESPONSABLE	ACTIVIDAD
Especialista en Adquisiciones	Envía un oficio y muestra física a control de calidad indicando que se realice los análisis de laboratorio
Auxiliar de laboratorio de MP	Realiza el Informe de Análisis **(**físico químico o comparativo) para conocer el cumplimiento de variables de calidad y entregar al Especialista de Control de Calidad MP.
Especialista de control de calidad de MP	Comparar Normas Internacionales e INEN, con las especificaciones y toma la decisión de aprobar o rechazar el material. E informar resultados al Especialista de Adquisiciones

4.3.- MODELO PETI

4.3.1.- Estrategia de tecnologías de Información

Las soluciones de Tecnologías de Información que se establecen, buscan mejorar los procesos internos de la empresa e involucrar la sistematización en algunos de sus procesos y la utilización de tecnología más avanzada para procesos que de alguna manera se encuentran automatizados. Además se cubrirán las necesidades puntuales que su sistema actual no las cubren.

La implementación de un sistema que permita la Comercialización Electrónica (Venta, Compra y Facturación), permitirá a Fame, tener una ventaja competitiva con respecto a la competencia.

El proceso del mantenimiento de los equipos de producción involucra la implementación de un software de control que permita la planificación y ejecución de mantenimientos preventivos y correctivos, además de generar reportes de eficiencia de producción de cada uno de los equipos.

Además se identifican todos los procedimientos informáticos para que la generación de reportes unificados de los diferentes módulos de los procesos automatizados garantizando al acceso a la información actualizada y de manera que cubra las necesidades de los usuarios.

4.3.2.- Arquitectura de los sistemas de información

La modernización de Fame es transcendental para su desarrollo empresarial; para lo cual se deben mejorar los procedimientos y automatizar el manejo y administración de la información tanto para la comercialización como para la ejecución de sus procedimientos internos.

Parte de esta modernización corresponde al sistema de comercialización electrónico, que permitirá realizar transacciones de compra y venta en línea, Con esta herramienta FAME, podrá expandir su mercado a nivel regional y cumplir así su objetivo principal, además ahorrará tiempo y mejorará sus procesos brindando una gran facilidad a sus clientes y manejo de sus proveedores.

Por otro lado, para controlar la productividad de su planta operativa Fame debe contar con un sistema automático, que permita proyectar de manera planificada los

mantenimientos de sus equipos y que generé reportes del porcentaje de eficiencia de cada equipo en sus procesos de producción. Con este control, se evitará que la planta no pueda cumplir con los tiempos de entrega debido a problemas operativos, y permitirá un mejor control de la producción y reducirá la subutilización o sobreutilización de los distintos equipo industriales.

Para mejorar el acceso a la información y la personalización de reportes requeridos, se debe interrelacionar las herramientas informáticas que posee actualmente FAME. Algunos de los reportes que genera el Sistema Baan, pueden ser integrados por la herramienta Qlink View para la personalización de reportes que ayuden a la toma oportuna de decisiones.

4.3.2.1.- Diseño Funcional del Sistema

Al sistema de Fame estará conformado por los siguientes subsistemas como se muestra en el diagrama 4.6:

- Sistema Baan
- Sistema 9000Doc
- Sistema StrategyLink
- Sistema Adam
- Sistema QlikView
- Sistema Comercio Electrónico.
- Sistema Control y Mantenimiento.

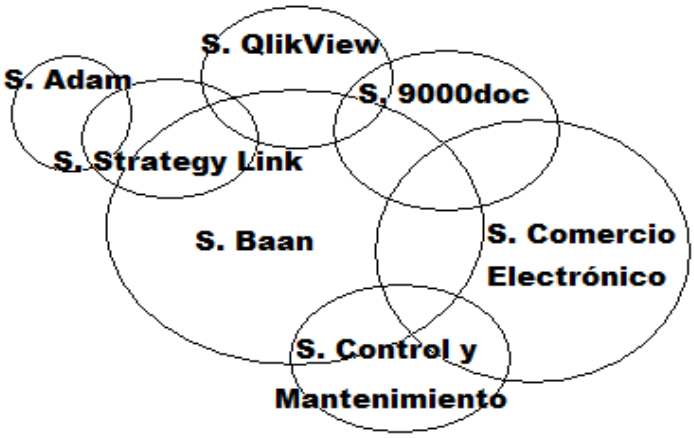


Diagrama 4.6 Sistema Integrado FAME

4.3.2.2.- Sistema Comercio Electrónico

El sistema de Comercio Electrónico debe permitir la compra, venta y facturación de manera electrónica., convirtiéndose en una herramienta de vital importancia para llevar a cabo el Proceso de Comercialización y Adquisición. Para esto, se deben desarrollar los diferentes módulos de acuerdo a la organización, los mismos deben estar entrelazados a fin de compartir la información administrativa y operativa.

Características del Sistema Comercio Electrónico

- Arquitectura escalable que permita aumentar la capacidad de servicio simplemente aumentando la capacidad hardware. La aplicación debe ser desarrollada en tres capas, con arquitectura orientada a servicios.

Diagrama 4.7 Arquitectura Orientada a Servicios.

- Aplicación desarrollada en ambiente 100% web que permita el acceso mediante navegadores que sea independiente de su plataforma base (sistemas operativos).
- Deberá permitir la manipulación de la información mediante herramientas de Gestión Gerencial para la toma de decisiones, estadísticas, reportes ejecutivos, etc.
- La aplicación debe ser multiplataforma y compatible con otras aplicaciones.
- Crecimiento ilimitado de usuarios.
- Acceso al sistema e ingreso de información desde cualquier parte del mundo.
- En línea 365/24/7.
- Recopilación en tiempo real de la información ingresada desde los sitios remotos.
- Presentación de reportes personalizados acorde a la necesidad de los usuarios, con formatos PDF, Excel, XML, etc.

- Perfiles de usuario para el acceso a módulos y manipulación de la información.
- Interfaz amigable para el usuario.
- Algoritmo eficiente de búsqueda y consulta de datos.
- Algoritmos de seguridad para transacciones bancarias y comerciales.
- Manejo de firmas electrónicas.

Funciones Operativas

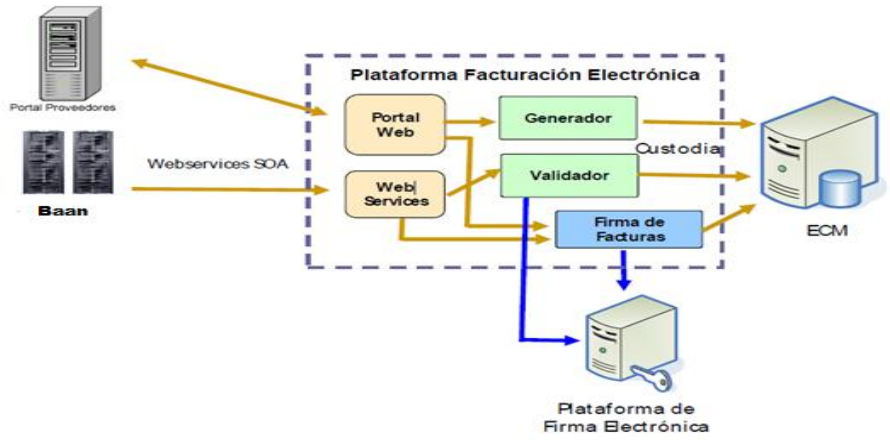


Diagrama 4.8 Arquitectura Sistema Comercialización

Portal Web

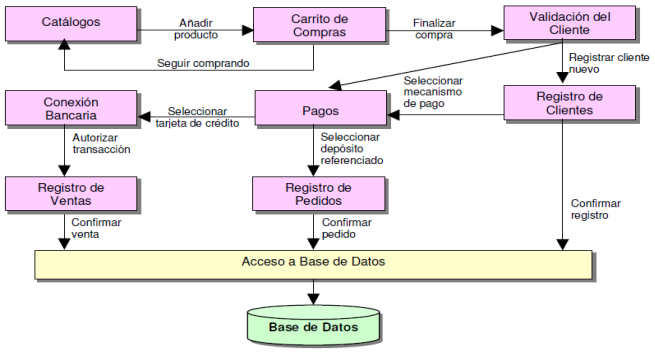


Diagrama 4.9 Arquitectura Portal Web

Módulo de Catálogos

En este módulo se incluyen las funciones de presentación y generación de catálogos de los productos de la tienda. Debido a que los catálogos de los productos se almacenan en la base de datos, este módulo realiza una consulta dinámica cada vez que se carga la página del catálogo, de tal forma que cualquier cambio en los catálogos se actualiza automáticamente. En el diagrama 4.10 se muestra el diagrama de este módulo.

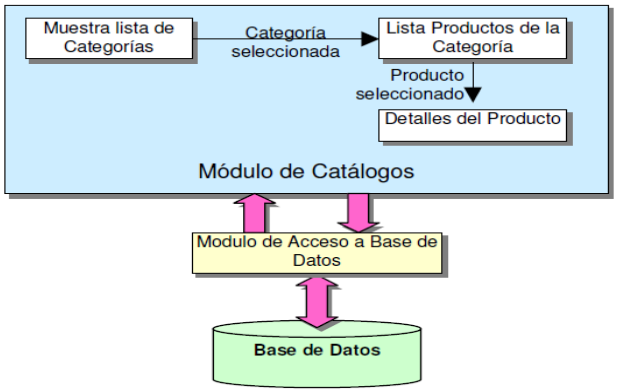


Diagrama 4.10 Módulo Catálogos

Módulo Carrito de Compras

Este módulo tiene la función de administrar los productos que el cliente desea comprar, manteniendo esta información en una sesión, hasta que el cliente decide realizar el pedido de los artículos o realizar el pago. Utiliza dos componentes, uno representa la estructura de los datos que se almacenan en el carrito; y el otro es una clase que implementa un vector en el cual se añaden y eliminan elementos del carrito. En el diagrama 4.11 se muestra el diagrama de este módulo.

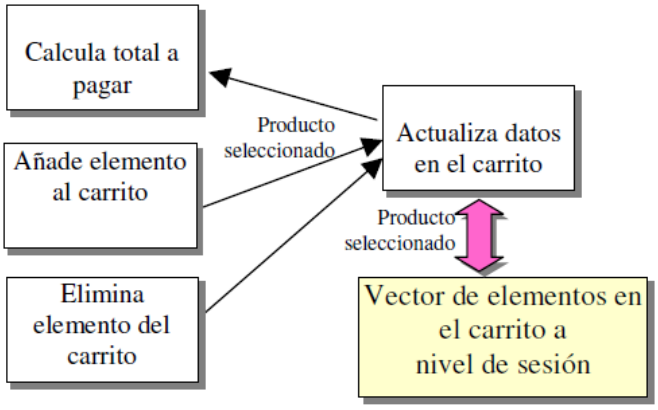


Diagrama 4.11 Módulo Carrito de Compras.

Módulo Registro de Clientes

Este módulo engloba todas las funciones necesarias para la identificación y registro del cliente. Toda la información del cliente se almacena en la base de datos, con el propósito de que el cliente no tenga que proporcionar sus datos cada vez que visita la tienda. En el diagrama 4.12 se muestra el diagrama de este módulo.

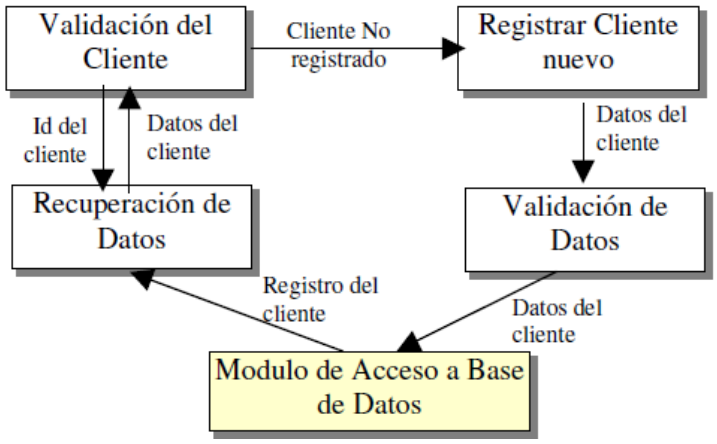


Diagrama 4.12 Módulo Registro Clientes

Módulo de Pagos

Este módulo tiene la función de presentarle al cliente las opciones de pago para que el cliente elija entre el pago con tarjeta de crédito o pago con depósito referenciado. En el diagrama 4.13 se muestra el diagrama de este módulo.

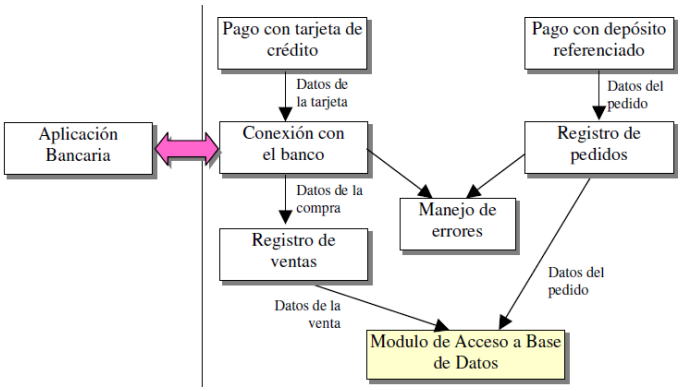


Diagrama 4.13 Módulo de Pagos

Pago con Depósito Referenciado

Cuando el cliente decide realizar su pago con depósito referenciado se genera de un número de pedido único y se registra el pedido del cliente en la base de datos. Posteriormente el cliente realiza el depósito llenando la ficha de depósito del banco que elija y anotando el número de referencia del pedido. Al momento de que el banco registra el número de referencia del depósito, la tienda puede acceder a la información de su cuenta bancaria y conocer quién hizo el depósito y a qué pedido le corresponde.

Pago con Tarjeta de Crédito

La autorización de la tarjeta de crédito es uno de los aspectos más oscuros del comercio electrónico. Es muy difícil encontrar información específica sobre el procedimiento de los bancos para aceptar tarjetas de crédito en línea. La mayoría de los bancos están conectados a redes que no funcionan sobre TCP/IP, usualmente están conectados mediante redes como X.25, frame relay, IPX, etc.

Para que la tienda tenga una comunicación con el banco, éste exige que la empresa solicitante sea legítima, y que implemente en su servidor Web mecanismos de seguridad como la encriptación de la transmisión de datos mediante el protocolo de seguridad SSL, y la obtención de un certificado público de autenticidad.

Conexión con el Banco

Este módulo establece una conexión con la interfaz bancaria mediante un canal de comunicación, a través del cual se envían los datos de la tarjeta para su autorización, y se recibe la respuesta que el banco envía.

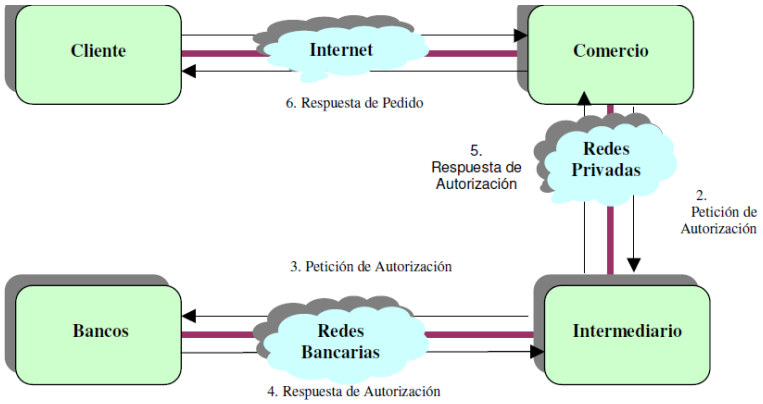


Diagrama 4.14: Conexión con Bancos

Web Services

Se desarrollaran o utilizaran Web Services que permitirán la comunicación entre aplicaciones o componentes de aplicaciones de forma estándar a través de protocolos comunes (como http) y de manera independiente al lenguaje de programación, plataforma de implantación, formato de presentación o sistema operativo. Un Web service es un contenedor que encapsula funciones específicas y hace que estas funciones puedan ser utilizadas en otros servidores.

Firma de Facturas

Permitirá que la o las personas responsables firmen digitalmente los comprobantes fiscales como facturas, retenciones, notas de ventas, etc. Para contar con una firma digital y las seguridades respectivas de ley, se contratará el servicio a una empresa CA: Autoridad Certificadora (Prestador de servicios de certificación).

Generador

Una vez implantados los servicios de firma electrónica para aplicaciones corporativas, para cumplir la normativa ecuatoriana de presentación de facturas en formato electrónico a las administraciones publicas se desarrollará o implantará una herramienta que permita convertir las facturas emitidas desde el sistema de gestión BAAN al formato facturae y que utilice los servicios la plataforma de firma para realizar el firmado de la factura según las políticas de firma definidas en la "Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos", para su posterior envío a los servicios que la administración facilite para las mismas.

La solución escogida para realizar estas tareas de emisión de facturas electrónicas debe proporcionar un interfaz único de emisión de facturas a los sistemas ERP corporativos, aislando la lógica de formateo y firma de la factura electrónica.

Además debe proporcionar un interfaz de entrada para facturas electrónicas de proveedores.

Debe tener un interfaz o un API para integrarse fácilmente con el sistema Baan, realizando el proceso de aprobación de facturas y posterior contabilización automática en el sistema de gestión.

Validador

Este módulo se encargará de comprobar que las firmas digitales sean autenticas, mediante la conexión y validación con la plataforma de firma electrónica.

Plataforma de Firma Electrónica

Esta plataforma será provista de un CSP/CA: Autoridad Certificadora (Prestador de servicios de certificación).

Portal Proveedores

Esta aplicación servirá para realizar los pedidos a los proveedores y que éstos ingresen sus respectivas facturas digitales para posteriormente se registrados y contabilizadas. Además generará los contratos de comercialización entre las partes.

4.3.2.3.- Sistema Control y Mantenimiento

- Debe ser desarrollado en ambiente web, compatible con todos los navegadores.
- La arquitectura debe ser entres 3 capas, orientada a servicios.
- Recopilación en tiempo real de la información ingresada desde los sitios remotos.
- Presentación de reportes personalizados acorde a la necesidad de los usuarios, con formatos PDF, Excel, XML, etc.
- Perfiles de usuario para el acceso a módulos y manipulación de la información.
- Interfaz amigable para el usuario.
- Algoritmo eficiente de búsqueda y consulta de datos.

Funciones Operativas

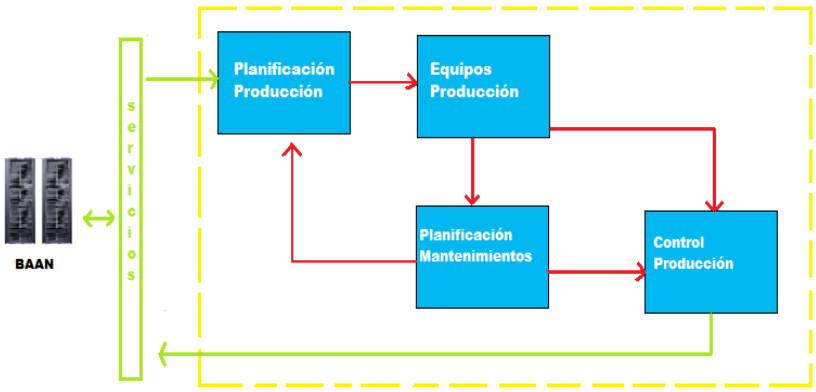


Diagrama 4.15 Arquitectura Sistema Control y Mantenimiento

Módulo de Planificación de Producción

Este módulo recibirá las órdenes de producción ingresadas en el BAAN, validará el estado de los equipos necesarios para la producción, el jefe de producción validará los parámetros necesarios para que el módulo calcule y genere la cola de pedidos de producción en cada uno de los equipos.

Módulo de Equipos Producción

En este módulo el operario de cada máquina tendrá en cola la lista de pedidos a producir, iniciará la producción del pedido y registrará en el módulo el tiempo de producción en el equipo, el tiempo que el equipo ha permanecido inutilizado en el proceso de producción y escogerá una causa (Daños, trabas, reparaciones, etc.). Además actualizará el porcentaje de avance de la producción del pedido asignado.

Planificación Mantenimientos

Este módulo contendrá los parámetros necesarios para la planificación de los mantenimientos preventivos y registrará cuando un equipo se encuentre en mantenimiento correctivo, esta información servirá para el módulo de Planificación de Producción y Control Equipos Producción.

Control Equipos Producción

Mediante este módulo, se podrá controlar el avance de los trabajos de producción en cada uno de los equipos, los mantenimientos preventivos y correctivos, además se podrá generar reportes de eficiencia de producción de cada uno de los equipos para la toma de decisiones.

4.3.2.4.- Generación de Reportes Personalizados

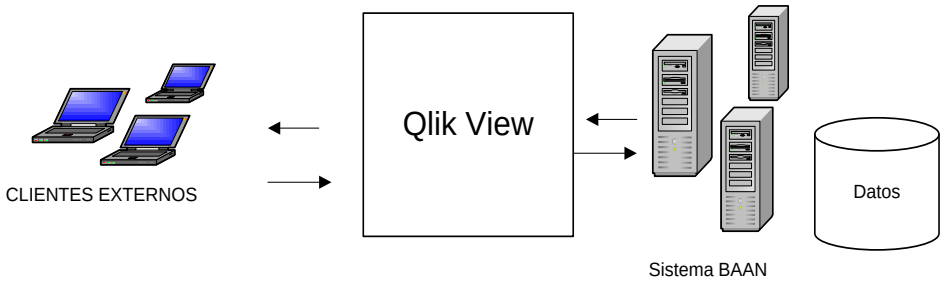


Diagrama 4.16 Arquitectura Integración Sw Baan y Sw QlikView

Debido a que algunos de los reportes que genera el ERP Baan no satisface las necesidades de ciertas áreas de Fame, y a que, cuentan con la herramienta de Bussines Intelligence Qlikview, se asignara a un ingeniero analista de sistemas para que enlace estas dos aplicaciones con la información necesaria para generar los reportes que no genere el Baan o no cumplan las exigencias de los departamentos de FAME.

Con el script de QlikView se accede a cualquier base de datos vía ODBC/OLE DB. Además, se integran diferentes formatos de ficheros planos: csv, xls, xml, qvw, etc. El script de QlikView incluye funciones potentes a la hora de depurar o manipular la entrada de datos. Se basa en un lenguaje propio, muy similar a SQL por lo que un desarrollador requiere muy poca formación para aprovechar al máximo todas las funcionalidades.

Las asociaciones entre los datos de diferentes tablas se crean en el momento de ejecución del script en la base de datos de QlikView, basándose en la lógica asociativa. QlikView utiliza para ellos campos clave que coinciden con los nombres idénticos de campos de diferentes tablas.

4.3.3.- Arquitectura de tecnología

La arquitectura de los sistemas a implementar debe ser orientada a los servicios y en tres capas. Una capa independiente de los servicios para interconectar las peticiones para las aplicaciones. Otra capa independiente de las aplicaciones y bases de datos existentes y finalmente la capa de los clientes.

Los usuarios externos se conectaran mediante el internet mientras que los usuarios internos lo harán a través de la intranet.

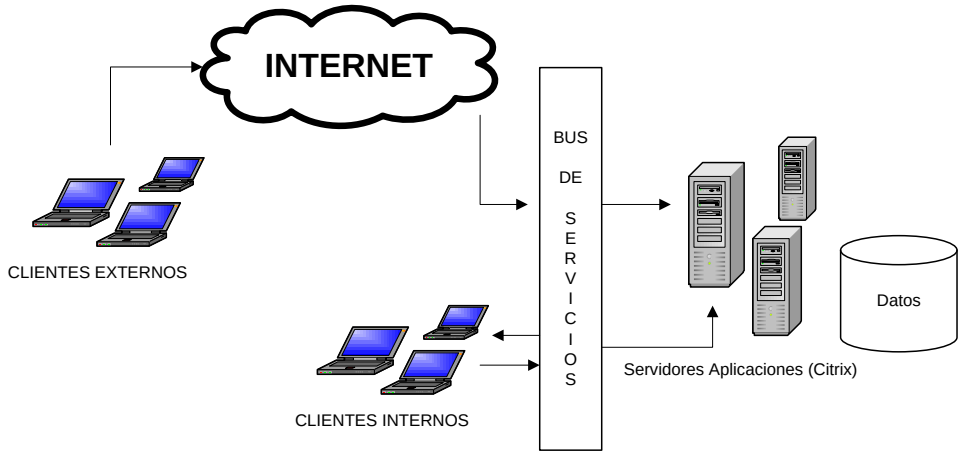


Diagrama 4.17 Arquitectura de TI

4.3.3.1.- Herramientas de Desarrollo

Se desarrollará en Java por ser un lenguaje multiplataforma y un estándar en las aplicaciones Web por su seguridad y cantidad de librerías que facilitan el trabajo de desarrollo, por tener conectividad con un gran número de bases de datos, se puede desarrollar con el IDE Jbuilder de Borland, Netbeans o Eclipse, que es una herramienta RAD para acelerar el desarrollo, se utilizará la última versión de Java.

4.3.3.2.- Comunicaciones

Fame, al pertenecer al grupo empresarial Holding Dine cuenta con una infraestructura completa de comunicaciones de datos con el edificio matriz.

Este servicio es provisto por la empresa Telconet. La última milla proporcionada es de fibra óptica y posee redundancia con radio enlace, con este mecanismo la empresa proveedora se asegura de mantener en línea los servicios de comunicación.

Internamente cuenta con un equipo Cisco 1811 que enlaza la red Wan con la red Lan de la empresa. La infraestructura de comunicaciones LAN es Gigabit Ethernet 10/100/1000.

La empresa Telconet, ofrece un servicio de internet de 1Gbs dedicado 1 a 1 sin comparticiones con lo que garantiza una excelente navegación.

Además tiene un Túnel de datos de 1048Mbs con el edificio Matriz, ofreciendo una comunicación fluida de datos.

La infraestructura actual cuenta con los requerimientos necesarios para ofrecer una buena transferencia de datos con los nuevos sistemas propuestas a implementar.

4.3.4.- Modelo operativo de tecnologías de información

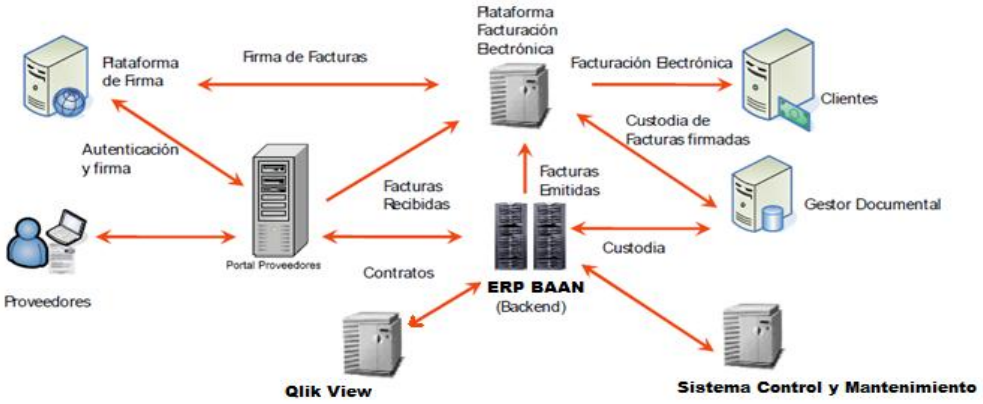


Diagrama 4.18 Modelo Operativo de TI

La plataforma de firma da servicios de autenticación y firma digital a las aplicaciones corporativas. En particular a la plataforma de facturación electrónica para la firma de facturas y al portal de proveedores para la autenticación de los mismos.

Por su parte, la plataforma de facturación estará integrada con el portal de proveedores para que estos puedan entregar las facturas digitales, con el BAAN para recibir las facturas que se van a emitir en formato electrónico (idealmente también para realizar la contabilización de las mismas en el backend), con la plataforma de firma para realizar la firma de las facturas entrantes y salientes y con el gestor documental para realizar la custodia de los documentos firmados.

El Software Qlik View se conecta con el Baan para la generación de reportes, mientras que el Sistema de Control y Mantenimiento intercambia información sobre el estado de los equipos de producción de la planta.

4.3.5.- Estructura organizacional deTI

ESTRUCTURA ORGANIZACIONAL PROPUESTA DE LA JEFATURA DE SISTEMAS DE INFORMACIÓN Y COMUNICACIONES

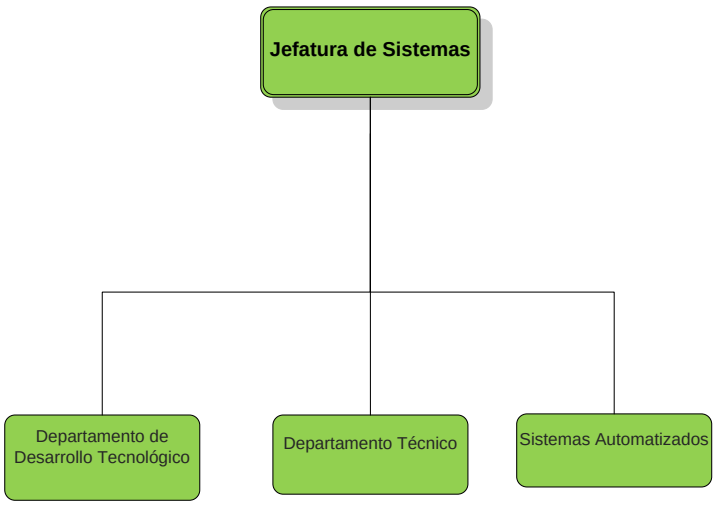


Diagrama 4.19 Estructura Organizacional

Para la estructura propuesta se necesita el siguiente recurso humano detallado a continuación

Tabla 4.41 Recurso Humano Departamento de Tecnologías de Información

ÁREA	**Nº**	**CARGO**	**PERFIL**
Jefatura de Sistemas	1	Jefe Sistemas	Ingeniero Sistemas
Departamento de Desarrollo Tecnológico	2	Analista Desarrollador Sistemas	Ingeniero Sistemas
Departamento Técnico	1	Técnico de Soporte	Tecnólogo Sistemas
Sistemas Automatizados	1	Analista de Sistemas	Ingeniero Sistemas
Total	6		

4.3.5.1.- Procesos del Departamento de TI

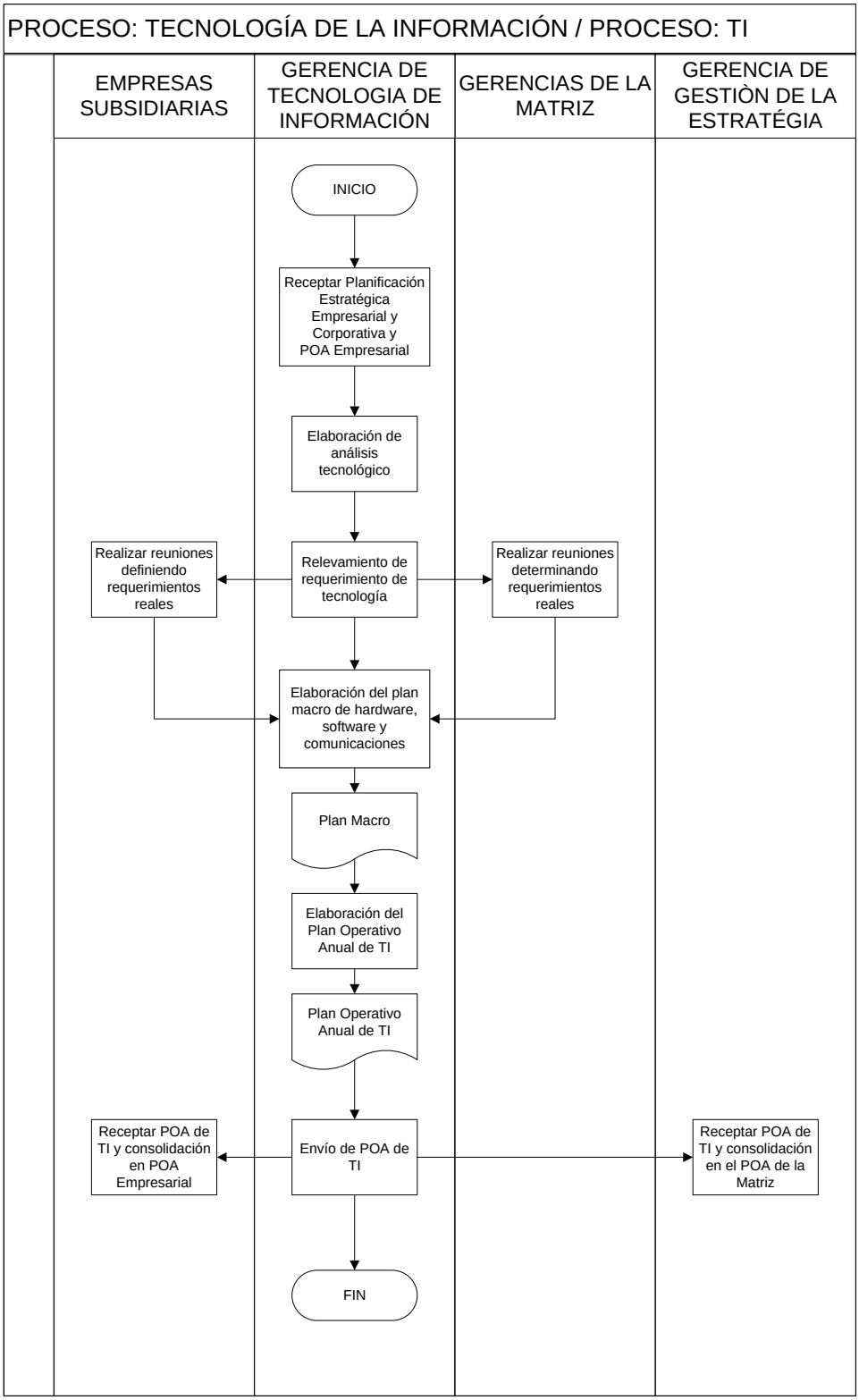


Diagrama 4.20: Proceso del Departamento de TI

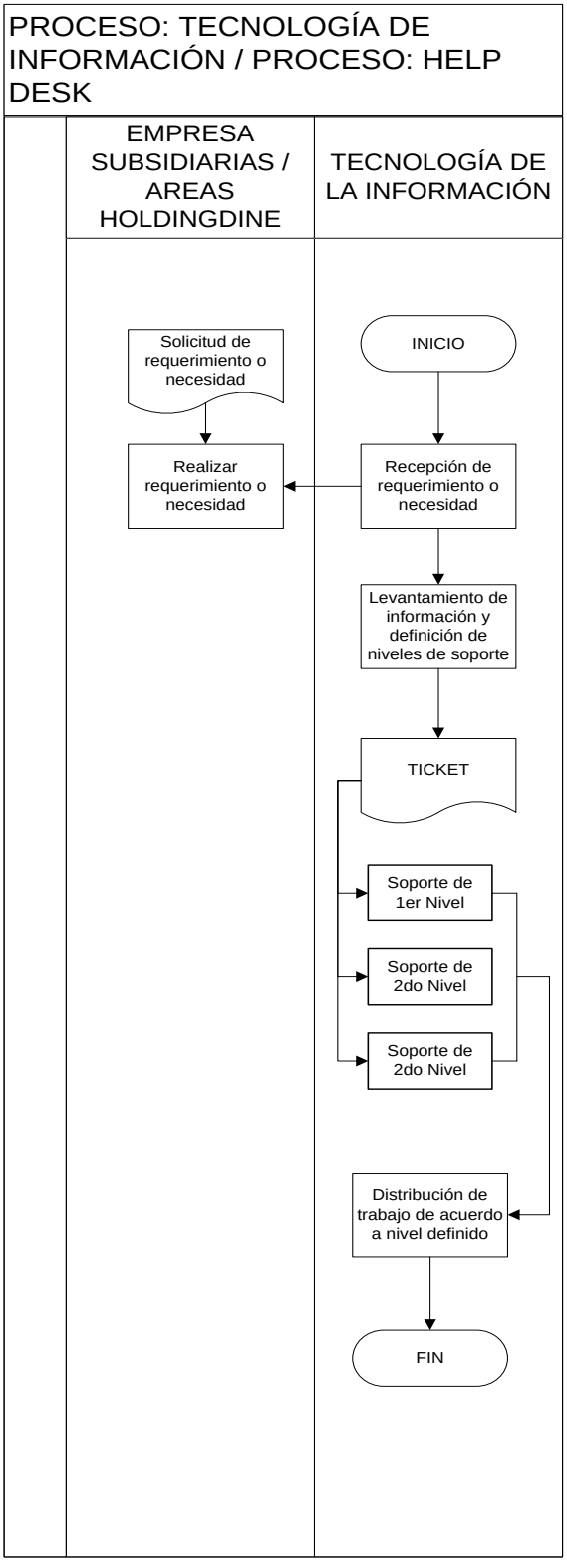


Diagrama 4.21: Proceso de Help Desk de TI

4.4.- MODELO DE PLANEACIÓN

4.4.1.- Prioridades de implantación

Para determinar la prioridad de desarrollo y de implantación se desarrolla la matriz de Holmes, se plantea los factores aspectos para el análisis:

- Procesos Automatizados
- Ampliación de Mercado
- Costo
- Tiempo de Desarrollo
- Transacciones en línea
- Apoyo a la Estrategia de Negocios
- Solución de Problemas Internos

Dichos factores serán comparados entre sí y serán calificados según su importancia. 1 Si el factor evaluado es relativamente más importante que su contraparte y 0 si el factor evaluado es relativamente menos importante que su contraparte.

Es necesario recalcar, que todas la calificaciones tienen un espejo, es decir, que las calificaciones que se pongan por encima de la diagonal principal necesitan ser correspondidas por debajo con su valor complementario.

Finalmente, la sumatoria de sus calificaciones nos dará su peso (%), para determinar su prioridad.

Tabla 4.42: Matriz de Holmes

	Autom.de Procesos	Ampliación de Mercado	Costo	Tiempo de Desarrollo	Transacciones en línea	Apoyo a la Estrategia de Negocios	Solución de Problemas Internos	Suma	Porcentaje de Impacto
Procesos Automatizados	0.5	0	1	1	1	0	0	3.5	14%
Ampliación de Mercado	1	0.5	1	1	1	1	1	6.5	25%
Costo	0	0	0.5	1	1	0	0	2.5	10%
Tiempo de Desarrollo	0	0	0	0.5	1	0	0	1.5	6%
Transacciones en línea	0	0	0	0	0.5	0	1	1.5	6%
Apoyo a la Estrategia de Negocios	1	0	1	1	1	0.5	1	5.5	22%
Solución de Problemas Internos	1	1	1	1	0	0	0.5	4.5	18%
							Total	25.5	

Tabla 4.43: Evaluación de Sistemas con Factores de importancia 1=bajo, 5 = alto.

	Automatización de Procesos	Ampliación de Mercado	Costo	Tiempo de Desarrollo	Transacciones en línea	Apoyo a la Estrategia de Negocios	Solución de Problemas Internos
Sistema Comercio Electrónico	3	5	5	5	5	5	2
Sistema Mantenimiento	5	2	3	3	1	2	4
Conectividad entre Baan y QlikView	2	1	2	2	1	2	5

Tabla 4.44: Evaluación de Sistemas con Peso de Factores de Importancia

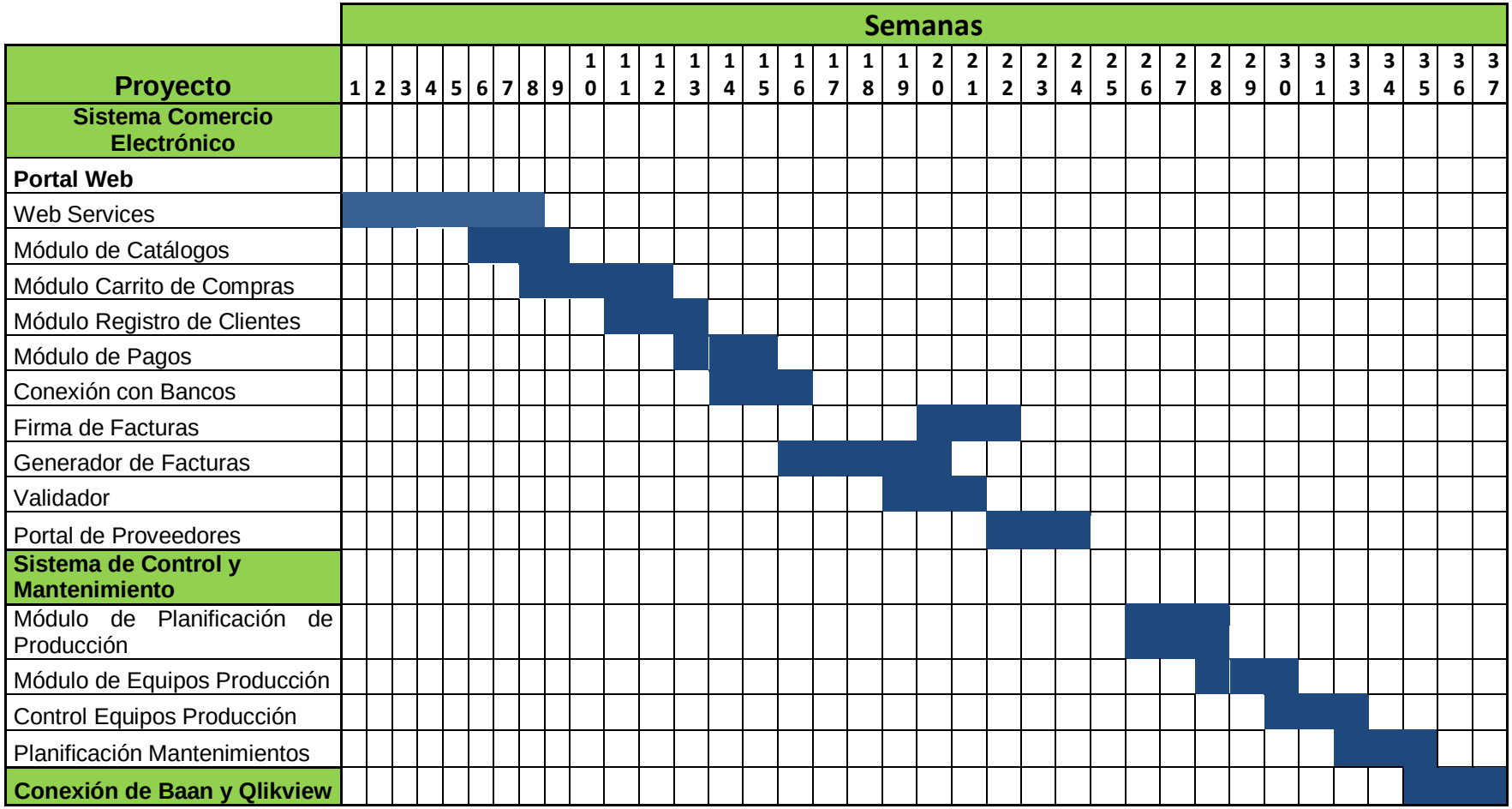
	Automatización de Procesos	Ampliación de Mercado	Costo	Tiempo de Desarrollo	Transacciones en línea	Apoyo a la Estrategia de Negocios	Solución de Problemas Internos	**Suma**
Sistema Comercio Electrónico	0.41	1.27	0.49	0.29	0.29	1.08	0.35	**4.20**
Sistema Mantenimiento	0.69	0.51	0.29	0.18	0.06	0.43	0.71	**2.86**
Conectividad entre Baan y QlikView	0.27	0.25	0.20	0.12	0.06	0.43	0.88	**2.22**

Como se puede apreciar en el análisis desarrollado con la Matriz de Holmes, las prioridades de implantación son las siguientes:

1. Sistema Comercio Electrónico
2. Sistema de Mantenimiento
3. Conectividad entre Baan y Qlikview

4.4.2.- Plan de implantación

Tabla 4.45: Plan de Implantación



4.4.3.- Retorno de la inversión

4.4.3.1 Costos

Tabla 4.46: Costos

Proyecto	
Sistema Comercio Electrónico	
Portal Web	
Web Services	$ 5,760.0
Módulo de Catálogos	$ 2,880.0
Módulo Carrito de Compras	$ 3,600.0
Módulo Registro de Clientes	$ 2,160.0
Módulo de Pagos	$ 2,160.0
Conexíon con Bancos	$ 2,160.0
Firma de Facturas	$ 2,160.0
Generador de Facturas	$ 3,600.0
Validador	$ 2,160.0
Portal de Proveedores	$ 2,160.0
Subtotal	**$ 28,800.0**
Sistema de Control y Mantenimiento	
Módulo de Planificación de Producción	$ 2,160.0
Módulo de Equipos Producción	$ 2,160.0
Control Equipos Producción	$ 2,160.0
Planificación Mantenimientos	$ 2,160.0
Subtotal	**$ 8,640.0**
Conexión de Baan y Qlikview	**$ 2,160.0**
Hardware	
Equipos Desarrollo	**$ 2,000.0**
Servidores	**$ 8,000.0**
Capacitación	**$ 2,000.0**
Subtotal	**$ 12,000.0**
Total	**$ 51,600.0**

Para calcular el presupuesto necesario en el desarrollo de los sistemas, se considera la contratación de dos desarrolladores con experiencia no junior durante la duración del proyecto con un costo por hora de $18 x h.

4.4.3.2 Beneficios

- Creación de canales nuevos de marketing y ventas.
- Acceso interactivo a catálogos de productos, listas de precios y folletos publicitarios.
- Venta directa e interactiva de productos a los clientes.
- Soporte técnico ininterrumpido, permitiendo que los clientes encuentren por sí mismos, y fácilmente, respuestas a sus problemas mediante la obtención de los archivos y programas necesarios para resolverlos.
- Incremento de un 15% al 30% en las ventas.
- Ahorro hasta un 3% en los costos administrativos.

4.4.3.3 Retorno de la Inversión

Fame tiene un promedio mensual de ventas de $1`000.000.

La rentabilidad promedio es de un 20%.

La utilidad mensual es de $200000 promedio.

La implementación de los sistemas propuestos bordea los $52000.

La facturación tendría un incremento mínimo del 3 al 10%, es decir se fijaría en $1`030.000 con una utilidad de $206000.

El excedente en la utilidad mensual sería $206000-$200000=$6000. Si este rubro se lo asigna para el financiamiento del proyecto, en aproximadamente 9.5 meses Fame recuperaría lo invertido.

4.4.4.- Administración de riesgo

La cambios que se generan en las organizaciones de manera rápida crean nuevos riesgos en el desarrollo e implementación de los Sistemas de Tecnología de Información, esto obliga a gestionarlos con cursos de acción y planes de contingencia para todos los sistemas y componentes considerados en la planificación del proyecto.

4.4.4.1 Identificación y Control de Riesgos

Una vez que se conozca de manera clara los riesgos potenciales que puedan generarse en el desarrollo del proyecto, entonces se analizarán estrategias de mitigación, planes de contingencia y sobre todo que estos riesgos no ocurran, lo que implicará los siguientes beneficios:

- Diagnóstico real de los problemas que se puedan presentar en el ambiente de desarrollo del proyecto.
- Conocer los problemas o inconvenientes que se puedan suscitar en los equipos informáticos, redes, usuarios, procesos administrativos y flujo de información.
- Efectuar el análisis de riesgos de todos los posibles problemas con su respectiva probabilidad de ocurrencia e impacta que pueda causar.
- Realizar contingencias una vez ocurridos los problemas o catástrofes.
- Capacitar al personal para enfrentar todo tipo de desastres naturales o accidentales.

- Establecer procedimientos para evitar las interrupciones prolongadas una vez suscitado el problema.

4.4.4.2 Clasificación e Identificación de los Riesgos

Se los clasifica e identifica en la tabla 4.47.

Tabla 4.47: Identificación de Riesgos

Clasificación	Tipo	Identificador	Descripción
A	Financiero/Económico	A.1	Inflación
		A.2	Recesión Económica
B	Diseño	B.1	Diseños Incompletos
		B.2	Mal Especificados
C	Físico	C.1	Daños en Instalaciones
		C.2	Falla de Equipos
D	Político/Entorno	D.1	Cambio de Leyes
		D.2	Requisitos y Aprobaciones
E	Sociales	E.1	Productividad
		E.2	Condiciones de Trabajo
F	Tecnológico	F.1	Evolución
		F.2	Obsolescencia
		F.3	Incompatibilidad
		F.4	Desarrollos Incompletos
		F.5	Formación
G	Interno	G.1	Cambios en la Estructura
		G.2	Modificación de la Estrategia
		G.3	Cambios Físicos

4.4.4.3 Ponderación, Probabilidad de Ocurrencia e Impacto de Riesgos

Es fundamental para el proceso de mitigación de riesgos determinar cuáles riesgos podrían llegar a tener un mayor impacto con su aparición durante el proceso de desarrollo del proyecto, es por esto que, surge la necesidad de establecer una unidad de medida que permita calcular la magnitud de los riesgos identificados.

Tabla 4.48: Ponderación de Riesgos

Puntaje	Calificación
81-100	Muy Alto
61-80	Alto
41-60	Medio
21-40	Bajo
0-20	Muy Bajo

En la siguiente tabla se establece las calificaciones a través de un sistema de puntaje para establecer el potencial impacto y probabilidad de ocurrencia de los riesgos clasificados anteriormente.

Tabla 4.49 Probabilidad de Ocurrencia e Impacto de Riesgos

Puntaje	Calificación	Probabilidad de Ocurrencia	Impacto de Ocurrencia
100	Muy Alto	Altamente Probable.	Mayor impacto. Implica 30% de Desviación
80	Alto	Probable	Alto Impacto. No llega al 30% de Desviación
60	Medio	Medianamente Probable	Medio. No afecta al cronograma
40	Bajo	Poco Probable	Bajo.
20	Muy Bajo	Muy poco probable	Muy Bajo. Insignificante

4.4.4.5 Análisis de Riesgos

Tabla 4.50 Análisis de Riesgos

Id.	Tipo	Descripción	Ocurrencia	Impacto	Prioridad (Ocu.+ Impac.)/2
A.1	Inflación	Las medidas monetarias del país afectan directamente al proyecto	60	100	80
A.2	Recesión Económica	Las constantes recesiones mundiales llevan al recorte de prepuestos	60	100	80
B.1	Diseños Incompletos	Falta de acceso a la información por parte de usuarios finales	80	90	85
B.2	Mal Especificados	Nuevos requerimientos luego de establecer el alcance del proyecto	100	100	100
C.1	Daños en Instalaciones	Falta de una infraestructura moderna para la implementación	60	80	70
C.2	Falla de Equipos	Equipos Obsoletos que no soportan nuevas tecnologías	40	80	60
D.1	Cambio de Leyes	Ajuste a nuevas leyes de comercio y control	60	90	75
D.2	Requisitos y Aprobaciones	Legislación monetaria extranjera	40	20	30
E.1	Productividad	Falta de capacitación en el uso de herramientas estándares	80	100	90
E.2	Condiciones de Trabajo	Falta de Infraestructura para el desarrollo de sistemas	80	100	90
F.1	Evolución	Falta de colaboración de Usuarios y Gerencia para pruebas del sistema	60	60	60
F.2	Obsolescencia	Tecnología Obsoleta	40	60	50
F.3	Incompatibilidad	Entre sistemas actuales	80	80	80
F.4	Desarrollos Incompletos	Estudios mal dimensionados y proyectos abandonados	90	100	95
F.5	Formación	Falta de capacitación en las herramientas de desarrollo	80	80	80
G.1	Cambios en la Estructura	Rotación de Puestos Gerenciales	80	90	85
G.2	Modificación de la Estrategia	Falta de apoyo al cambio a nuevas tecnologías	60	60	60
G.3	Cambios Físicos	Cambio de oficinas o apertura de nuevas sucursales	40	20	30

Tabla 4.51 Métodos para Combatir el Riesgo

Riesgo	Prioridad	Métodos para combatir el riesgo
Nuevos requerimientos luego de establecer el alcance del proyecto	100	Establecer un alcance real del proyecto que contemple todos los requerimientos
Estudios mal dimensionados y proyectos abandonados	95	
Falta de capacitación en el uso de herramientas estándares	90	Medir la capacidad del recurso humano y de infraestructura antes del inicio del proyecto
Falta de Infraestructura para el desarrollo de sistemas	90	
Falta de acceso a la información por parte de usuarios finales	85	Asegurar y legalizar por escrito el Ok de Gerencia
Rotación de Puestos Gerenciales	85	
Las medidas monetarias del país afectan directamente al proyecto	80	Asegurar partidas presupuestarias. Analizar inversiones de terceros
Las constantes recesiones mundiales llevan al recorte de prepuestos	80	
Incompatibilidad entre sistemas actuales	80	Verificar compatibilidad de Sistemas con herramientas de desarrollo
Ajuste a nuevas leyes de comercio y control	75	Asegurar partidas presupuestarias. Analizar inversiones de terceros
Falta de una infraestructura moderna para la implementación	70	Estudio de Infraestructura
Equipos Obsoletos que no soportan nuevas tecnologías	60	
Falta de colaboración de Usuarios y Gerencia para pruebas del sistema	60	Asegurar y legalizar por escrito el Ok de Gerencia
Falta de apoyo al cambio a nuevas tecnologías	60	
Tecnología Obsoleta	50	Estudio de Infraestructura
Legislación monetaria extranjera	30	
Cambio de oficinas o apertura de nuevas sucursales	30	

CAPÍTULO V

PLAN DE SEGURIDAD INFORMÁTICA

5.1.- ANTECEDENTES

Debido a la falta de procedimientos y el interés en mejorar el tema de seguridad de la información por parte del complejo Fabril FAME, se ha definido una política de seguridad en la cual se dará las recomendaciones necesarias para no poner en riesgo y/o eliminar las amenazas actuales.

5.2.- OBJETIVO

Elaborar un plan de seguridad informática para el Complejo Fabril FAME, en el cual se establecerán las guías a seguir, para implantar un modelo de seguridad de la información mediante la concientización del personal.

5.3.- ALCANCE

El presente documento está basado en los controles de la norma ISO 27002, para poder proteger de manera correcta la información de la organización; es de carácter global, es decir para todo el personal del Complejo, Proveedores, etc. Quienes deberán acatar todo lo expuesto.

5.4.- CONTENIDO Y DESARROLLO

El plan de seguridad informática hará referencia a los 11 dominios que la norma ISO 27002 abarca, los mismos que son:

- Política de seguridad
- Aspectos organizativos de la seguridad de la información
- Gestión de activos
- Seguridad ligada a los recursos humanos
- Seguridad física y ambiental
- Gestión de comunicaciones y operaciones
- Control de acceso
- Adquisición, desarrollo y mantenimiento de sistemas de información
- Gestión de incidentes en la seguridad de la información
- Gestión de la continuidad del negocio
- Cumplimiento

5.5.- POLÍTICA DE SEGURIDAD

5.5.1.- Política de Seguridad de la Información

5.5.1.1.- Documento de política de seguridad de la información

El Gerente General de FAME deberá realizar una revisión de las normas de seguridad vigentes, aprobarlas e implementar este documento de políticas de seguridad de la información, el cual tratara de contrarrestar las falencias presentadas al momento. El mismo deberá ser adoptado de manera inmediata y obligatoria; además de difundido a todo el personal de la empresa.

El documento de política de seguridad de la información contendrá:

- Definición, metas y objetivos de la seguridad de la información y su importancia dentro de la institución.
- Compromiso de la dirección de FAME para apoyar la gestión de seguridad de la información, siguiendo las estrategias del negocio.
- Definición de los objetivos de control y controles, y la gestión de riesgo.
- Planteamiento y explicación de las normas y políticas de la seguridad de la información.
- Nombramiento del personal encargado de la gestión de seguridad de la información.
- Documentación que respalde a la política de seguridad establecida.

Se deberá notificar a los encargados de cada departamento de FAME la política de seguridad de la información, para un posterior cumplimiento de cada uno de los controles establecidos.

De igual forma, esta política deberá ser comunicada al Departamento de Tecnología e Información de Holding Dine para sugerir su análisis e implementación en el grupo de empresas que lo conforman, como herramienta para optimizar la seguridad de la información.

5.5.1.2.- Revisión de la política de seguridad de la información

El presente documento deberá revisarse cada 4 meses para asegurar el cumplimiento del mismo por el personal a cargo. El responsable de esta revisión estará a cargo del Director del Departamento de Tecnología e Información y

Comunicación, junto con los responsables del Departamento de Seguridad Industrial de FAME.

El objetivo de esta revisión es ver la eficiencia de la política, así como establecer cambios que promuevan la correcta gestión de la seguridad de la información.

5.6.- ASPECTOS ORGANIZATIVOS PARA LA SEGURIDAD DE LA INFORMACIÓN

5.6.1.- Organización Interna

5.6.1.1.- Compromiso de la Dirección con la Seguridad de la Información

Es condición sine qua non que el Directorio del Complejo FAME y de ser necesario junto con el directorio de Holding Diñe, realicen reuniones periódicamente en las cuales revisen la política de seguridad de la información; apoyen la gestión de la misma, lo cual consistirá en dar seguimiento al cumplimiento de los controles en cada uno de los departamentos. De igual manera, se deberá asignar funciones y responsabilidades.

La Dirección deberá proporcionar todos los recursos necesarios para garantizar que la seguridad de la información sea efectiva, deberá fomentar la concientización del personal en cuando a seguridad de información mediante programas de capacitación.

5.6.1.2.- Coordinación de la seguridad de la información

En lo que respecta a coordinación de seguridad de la información, cada uno de los jefes de departamento, así como el personal designado previamente por el directorio tendrán que velar por la gestión de la seguridad de la información.

Deberán garantizar que las actividades de seguridad se ejecuten acorde a las políticas de seguridad, informar si no se está cumpliendo con lo establecido; analizar si existen nuevas amenazas, aportar con ideas para nuevos procedimientos de seguridad de información, incentivar al personal a conocer más acerca del tema y lo importante y riesgoso que es no tomarlo conscientemente.

La información destinada al personal de cada departamento será difundida por cada Jefe o encargado, y este a su vez a través de reuniones dadas junto con el directorio.

5.6.1.3.- Asignación de responsabilidades relativas a la seguridad de la información

Toda actividad referente a seguridad de la información debe estar asignada a una o varias personas o comité conformado, la o las mismas serán encargadas de hacer el seguimiento respectivo para futuras validaciones; estos encargados a su vez podrán sub designar a otras personas pero ante cualquier acontecimiento ellos serán los primeros responsables.

Todo proceso o procedimiento, debe estar definido claramente y por lo tanto documentado; es primordial que las tareas o actividades de cada uno de los procedimientos, sean asignadas a personal que se encuentre capacitado para poder

ejecutarlas y que sean conscientes de lo importante que es gestionar la seguridad de la información.

Además se deberá tomar en cuenta cada uno de los activos de la empresa, los mismos deberán tener un responsable, quien si bien es cierto puede o no hacer uso de dicho activo, deberá estar pendiente de su correcto manejo y funcionamiento.

5.6.1.4.- Proceso de autorización de recursos para el procesado de la Información

El Complejo deberá tener por escrito un procedimiento el cual defina los pasos a seguir si se presentan nuevos recursos de procesamiento de información; entre los pasos a seguir deberá constar:

- Todo nuevo Hardware o Software no podrá entrar directamente al departamento o equipo que lo vaya a utilizar, el encargado de seguridad de información de dicho departamento deberá realizar revisiones trimestralmente para detectar que equipos y que sistemas están siendo usados o van a ser usados sin conocimiento y permiso del directorio.
- Una vez que esto se detecte se informara al encargado del departamento, de igual manera, el personal que ingrese con equipos o sistemas ajenos.
- El Jefe de departamento deberá comunicar al departamento encargado de gestión de equipos y sistemas, en este caso el Departamento de Tecnología e Información, el cual hará un chequeo del recurso, y validara si no representa una amenaza para la información de la institución, así como que no presente incompatibilidades y posibles daños al resto de activos.

- El Departamento de Tecnología e Información, presentara un informe al Jefe del departamento que hizo el pedido de revisión, en el cual constara si lo analizado traerá o no consecuencias.
- El Jefe del departamento previo análisis al informe dará la autorización respectiva al uso del equipo o sistema, caso contrario dictara el no uso de los mismos.

5.6.1.5.- Acuerdos de confidencialidad

El Comité encargado de gestionar la seguridad de la información, deberá tomar acción sobre lo que son los acuerdos de confidencialidad existentes y modificarlos si es el caso.

Los acuerdos de confidencialidad deben estar comprometidos con el plan de seguridad de información, deben contener algunos puntos importantes los cuales se detalla:

- Estructura y términos que cumplan con las leyes implantadas por el estado
- Información acerca de lo que se va o quiere proteger
- Duración del acuerdo de confidencialidad o aclaración de confidencialidad absoluta indefinida
- Acciones a tomar una vez terminadas funciones o proyecto
- Sanciones en el caso de no cumplir el esquema de no divulgación

En el caso de un acuerdo de confidencialidad o no divulgación se puede tener encuentra muchos otros puntos, los mismos deberán cumplir con los requisitos de

seguridad no solo de información, pero deberán estar acorde a las políticas generales de la empresa.

Estos acuerdos se tendrán que revisar periódicamente para poder actualizarlos en el caso de que nuevas políticas de seguridad estén vigentes.

5.6.1.6.- Contacto con las autoridades

Es necesario que tanto el Complejo como su personal conozcan del acercamiento y resguardo con el que se cuenta por parte de las autoridades militares y policiales en el caso de que algún suceso ocurra dentro de la organización.

Esta información debe ser administrada por el Departamento de Responsabilidad Social, y son los mismos los que deben proveer del procedimiento a seguir para saber cómo actuar y como notificar incidentes identificados con respecto a la seguridad de la información.

Si las amenazas presentadas son ataques provenientes del internet, existe el debido contacto con sus proveedores para ejecutar sus planes de defensa y seguimiento.

El departamento en el cual se presenten las amenazas, deberá comunicarse de inmediato con el Departamento dde Tecnología e Información para que sea él el que tome en sus manos el análisis de la situación y siga el procedimiento de resguardo.

5.6.1.7.- Contacto con grupos de interés

Es necesario que el complejo FAME posea a parte de sus comisiones internas encargadas de la seguridad de la información, relaciones con instituciones o personal externos a la empresa especializados en seguridad de la información, para así poder recibir asesoramiento.

Es oportuno también que con estos vínculos se pueda compartir e intercambiar información acerca de temas actuales concernientes a vulnerabilidades y amenazas informáticas.

5.6.1.8.- Revisión independiente de la Seguridad de la Información

Se deberá realizar anualmente una auditoría con personal interno (distinta área a la evaluada) y externo a la empresa, los cuales validen que la gestión de la seguridad de la información funcione adecuadamente. Los informes presentados como resultado de la auditoría deberán ser reportados a la dirección y evaluados para forjar acciones correctivas en los objetivos o metas de la seguridad de la información en el caso de necesitarlo.

Si es el caso de una auditoría externa, el directorio del complejo FAME deberá solicitar la misma al directorio de Holding Diñe, el cual junto con el Departamento de Tecnología e Información darán la aprobación respectiva.

5.6.2.- Terceros

5.6.2.1.- Identificación de los riesgos derivados del acceso a terceros

En caso de ser necesario el acceso a áreas de procesamiento de información dentro de la empresa por parte de entidades externas, es necesario que se realice una evaluación de los posibles riesgos a los cuales el complejo FAME estaría expuesto y se documente.

Dentro de estos riesgos se deberá tomar en cuenta los equipos y sistemas a los cuales se tendrá acceso, el tipo de información que la entidad externa requerirá, la identificación del personal externo autorizado al acceso, el tratamiento de la información, entre otros.

Es primordial como segundo paso a seguir luego del análisis de riesgos, proceder a la firma del documento de confidencialidad y no divulgación (referirse al control: acuerdos de confidencialidad).

Finalmente al tratarse de temas como relaciones profesionales con entidades externas, las mismas deberán ser aprobadas por el directorio del complejo FAME y su Departamento Legal. En cuanto a instalaciones tecnológicas, se deberá tratar el asunto en conjunto con el Departamento de Tecnología e Información.

5.6.2.2.- Tratamiento de la seguridad con relación a los clientes

Respecto al acceso a los activos o información del complejo FAME por parte de los clientes, es necesario desarrollar procedimientos, los cuales se refieran a protección de activos (información, equipos, software), impedimento de copia y

divulgación de información, políticas de control de acceso (referirse a control: controles físicos de entrada).

De igual manera el cliente contará con servicios por parte del complejo FAME como protección de datos personales, de trabajos en común e información solicitada por el cliente.

5.6.2.3.- Tratamiento de la seguridad en contratos con terceros

La seguridad dentro de contratos con entidades externas es un tema, que debe ser considerado importante y delicado; el complejo FAME tiene un estándar de contratos en donde se manejan términos legales para hacerlos validos ante las leyes del estado, así mismo se especifica las tareas a realizarse por parte del contratado; sanciones en caso de no cumplir o satisfacer los requerimientos y de igual manera al no cumplir con tiempos establecidos, clausulas de confidencialidad y no-divulgación; en conclusión, el modelo de contratos es el estándar que se maneja se podría decir universalmente.

Debido a que el complejo no cuenta con un documento de políticas de seguridad de la información, estos contratos no contemplan puntos que hacen referencia a la seguridad de la misma; por lo tanto se dictara de manera general algunas de las clausulas que deben ser consideradas.

- Controles de acceso
- Controles que aseguren la seguridad de los activos físicos y lógicos de la institución.
- Restricciones a la copia de información.

- Destrucción de material utilizado por la entidad externa, al cabo de cumplido el contrato
- Métodos de instalación de hardware y software
- Montaje de escenarios aislados del trabajo diario de la organización, para que así no existan amenazas a la información del complejo
- Procesos claros y específicos para la gestión de cambios
- Procedimientos claros y específicos en cuanto a transferencia o cambio de personal, así como acuerdo de confidencialidad con cada integrante del equipo
- Procedimiento que garantice la continuidad del negocio o servicio en caso de cualquier imprevisto
- Derechos de monitoreo y auditoria por parte del personal interno del complejo a las tareas diarias que este ejecutando la entidad contratada
- Renegociación en caso de existir cambios durante el proceso de de ejecución del contrato.

Todo lo mencionado es como se dijo de carácter general, pero tienen por obligación constar dentro de un contrato y deberán ser desarrollados para que no existan dudas y no se omita cualquier paso dentro de los mismos.

Es necesario que la empresa contratada tenga la capacidad de garantizar que todo lo establecido en el contrato se cumpla, y tanto el personal externo como el personal interno se encargaran de escalar a los encargados del proyecto si existen irregularidades.

5.7.- GESTIÓN DE ACTIVOS

5.7.1.- Responsabilidad sobre los activos

5.7.1.1.- Inventario de activos

El Complejo FAME actualmente maneja su inventario de activos, el mismo posee información propia del activo, así como la persona a cargo y ubicación.

El implementar el uso de un inventario de activos, es de suma importancia y debe ser tomado muy en cuenta, todos los activos de la empresa deben ser identificados y tratados de acuerdo a su nivel de importancia; cada activo deberá tener código, nombre, lugar de ubicación, encargado, funcionalidad, licencias, costos, e importancia para el negocio.

Cuando se habla de activos no se hace referencia únicamente a equipos que se encuentran instalados el complejo, sino a todo lo que se posee entre estos:

- De Información: Bases de datos, Archivos de datos, etc.
- De Documentación: Manuales de usuario, Manuales de operación, Procedimientos, etc.
- De Software: Software de aplicación, software del sistema, herramientas de desarrollo, etc.

El Director o encargado del Departamento de Tecnología e Información, deberá tener al menos una copia de este inventario, el cual deberá ser actualizado trimestralmente. El inventario de activos permitirá al complejo no solo tener identificado sus recursos sino que permitirá dar la seguridad física necesaria para cada uno de ellos

5.7.1.2.- Responsable de los activos

Una vez identificados y clasificados los activos del complejo, es necesario que todos y cada uno de ellos sea designado a una o varias personas escogidas por el directorio, mediante un documento.

La o las personas designadas para ser responsables de los activos del complejo, deberán garantizar su cuidado, funcionamiento, protección; así como estar al tanto de las políticas de control de accesos con las cuales velaran por accesos autorizados a los activos bajo su cargo.

5.7.1.3.- Acuerdos sobre el uso aceptable de los activos

El Complejo FAME cuenta con la documentación adecuada en la cual constan las normas a seguir para el correcto uso de la información y de los activos como ejemplo: Reglas para el uso de correo electrónico e Internet; lineamientos para el uso de dispositivos móviles, entre otros. Se deberá revisar el documento existente y analizarlo, con el fin de validar si el documento cumple con estrategias de seguridad de la información.

Si el documento actual no cumple con la seguridad de la información, son los directivos del o los departamentos quienes deberán realizar los cambios necesarios; los mismos deberán realizar reuniones periódicas en intervalos de no más de seis meses; para que así las estrategias o lineamientos tengan cierto tiempo para que el personal se adapte y semestralmente se realicen cambios si así se requiere.

El documento ya terminado deberá ser difundido y aclarado a todo el personal del complejo y así certificar que todos y cada unos de los integrantes de FAME

conocen y son conscientes de que tipo de uso y cuán importante es la información y los activos presentes.

5.7.2.- Clasificación de la información

5.7.2.1.- Directrices de clasificación

En necesario que el complejo maneje de manera correcta la clasificación de la Información, actualmente se trabaja en cuatro niveles que son:

- Publica
- Secreta
- Secretísima
- Confidencial

La clasificación de la información debe ser de acuerdo a su impacto sobre la organización o negocio, integridad y disponibilidad.

El complejo debe manejar un documento en el cual se definan los niveles ya mencionados, y en el mismo debe estar claro el por qué de cada clasificación, como clasificar, reclasificar y el cuidado que se debe tener al momento de etiquetar la información.

El complejo puede contratar a personal externo el cual sea experto en seguridad de la información, para auditar y clasificar de manera adecuada la información; si el complejo dispone de personal con el conocimiento necesario, pues deberá lo más pronto posible proceder con la revisión y reclasificación de la

información. Serán los mismos aquellos que periódicamente ejecutaran revisiones para mantener actualizada la protección de la información.

Se recuerda que toda información la cual haya sido divulgada con o sin intención, deberá ser reclasificada, ya que la protección de la misma es innecesaria y puede incurrir en costos adicionales.

5.7.2.2.- Marcado y tratamiento de la información

Tomando en cuenta el control de directrices de clasificación, es necesario elaborar documentos los cuales especifiquen el procedimiento a seguir para el etiquetado, procesamiento, almacenamiento, transmisión, destrucción segura de activos, etc. De igual manera en estos procedimientos debería constar el etiquetado y manejo de información a compartirse con entidades externas.

El etiquetado consiste en rotular los activos sean físicos, lógicos o electrónicos según las directrices de clasificación, ahora bien existen activos de información que no es posible marcar físicamente con una etiqueta por lo cual se deberá buscar el medio electrónico para hacerlo; colocando labels en documentos o presentaciones, designando nombres sin permiso de cambio, estableciendo meta datos, etc.

Ahondando mas en el tema de cómo rotular los activos de la información, nombramos algunos de los posibles formatos de etiquetamiento:

- Todo documento deberá ser puesto al interior de una carpeta o folder, si se desea mas orden y control de distinto color diferenciando los niveles de clasificación de la información según las políticas del Complejo FAME; además deberá tener una etiqueta con su correspondiente categorización,

por ultimo deberán ser colocados en lugares seguros de igual manera dependiendo de su tipificación y custodiada por personal si fuese necesario.

- Todo equipo el cual contenga información con alto nivel de resguardo, deberá ser etiquetado con su tipificación, de igual manera deberá ser ubicado en un lugar especial con los debidos controles de acceso, y custodiado por personal si es necesario.
- Todo documento electrónico deberá tener al menos un label en su interior el cual identifique el nivel de clasificación que tiene la información que está tratando; su nombre deberá tener un indicio de su categorización y deberá tener los permisos necesarios para que solo su portador pueda administrar dicha información.
- En cuanto a medios que contengan información digital como discos duros, memorias extraíbles, diskettes, casetes, cd's; serán tratados que cualquier otro activo físico, tendrán una etiqueta con su clasificación, deberá ser resguardada por el personal a cargo, si es necesario su almacenamiento físico, pues tendrán un lugar en el Complejo, que tenga controles de acceso adecuados y en su preferencia que esta información tenga formato encriptado en los medios.

Toda información cuya clasificación sea de de secreta, secretísima y confidencialidad deberá ser tratada con suma delicadeza, y para poder ser intercambiada con personal el cual no sea el directo a cargo, pues se deberá tener una autorización dada por la gerencia o directorio del complejo FAME.

5.8.- SEGURIDAD LIGADA A LOS RECURSOS HUMANOS

5.8.1.- Seguridad en la definición del trabajo y los recursos

5.8.1.1.- Inclusión de la seguridad en las responsabilidades laborales

Es necesario que tanto empleados como usuarios externos que ejecutan actividades dentro del complejo FAME, tengan presente cuáles son sus funciones y responsabilidades.

Para poder brindar seguridad a la información es de suma importancia que se elaboren planes de capacitación para el personal, cursos de actualización, etc. Con lo cual se podrá minimizar el riesgo que actualmente FAME tiene en cuanto a desconocimiento del personal de la importancia de la seguridad de la información.

Para el complejo FAME será necesario definir en el documento de requerimientos para calificar o seleccionar a futuro personal, reglas y políticas que aclaren al o los candidatos cual será su rol, sus funciones y sus responsabilidades, esto deberá ser desarrollado en conjunto entre el Departamento de Recursos Humanos y el Departamento de Tecnología e Información, para así poder definir claramente los estándares de seguridad a ser cumplidos.

5.8.1.2.- Selección y política de personal

Actualmente el complejo FAME mantiene un estándar de contratación muy parecido a muchas otras empresas, el cual consiste en toma de pruebas de aptitud y conocimiento y se da seguimiento del perfil del candidato.

Es necesario, que la verificación de datos de todos los candidatos sean de acuerdo a los reglamentos establecidos por el complejo, que los candidatos sean

informados de las responsabilidades que van a asumir así como el riesgo y consecuencias de fallar ante alguna de ellas.

Este procedimiento de selección de personal, deberá ser llevado con suma delicadeza ya que de eso dependerá que el cargo a ser llenado se maneje de manera correcta y si por a o b dicho cargo manejara información sensible, pues del proceso penderá que no se presenten amenazas con el candidato seleccionado y por obvias razones el análisis y estudio del candidato deberá ser más detallado.

5.8.1.3.- Términos y condiciones de la relación laboral

Para lo que respecta a las condiciones y términos laborales, pues es requisito que la persona seleccionada firme el contrato de confidencialidad para así minimizar y tratar de controlar la fuga de información.

Por otro lado se deberá firmar el contrato el cual actualmente deberá ser revisado por personal del Directorio del complejo FAME, Recursos Humanos y Tecnología e Información para así actualizarlo y tomar en cuenta todo lo que respecta a seguridad de la información; en el mismo contrato se deberá establecer sus responsabilidades laborales, activos a su cargos, áreas de acceso y aclarar en su totalidad al candidato cual es su rol dentro de la organización.

5.8.2.- Seguridad en el desempeño de las funciones del empleo

5.8.2.1.- Supervisión de las obligaciones

Es obligación del directorio del complejo FAME realizar un seguimiento del personal nuevo, verificar si están de acuerdo con lo establecido en su contrato, si apoyaran la gestión de seguridad de información y de igual manera deberán exigir el cumplimiento de todas las políticas y procedimientos de seguridad.

Por otro lado es responsabilidad de la dirección del complejo que todo el personal este correctamente informado sobre las funciones y responsabilidades respecto a seguridad de la información, antes de asignar accesos a información.

El directorio deberá incentivar al personal para que el mismo logre concientizarse al máximo sobre la seguridad de la información y lo importante de la misma, de acuerdo a las políticas del complejo.

5.8.2.2.- Formación y capacitación en seguridad de la información.

Como otra de las responsabilidades del directorio de FAME con respecto a la seguridad de la información, pues está el hecho de planificar cursos y capacitaciones en las cuales se ensene de manera correcta el tema de seguridad de la información.

Para despertar el interés del personal en este tema, es necesario que no solo se tope el tema de gestión de seguridad dentro del complejo FAME, sino también fuera del mismo es decir en sus hogares por ejemplo:

- Instalación de virus en sus pc’s personales
- Evitar Pornografía adolescente
- Uso adecuado de redes sociales

- Configuraciones de seguridad para el Internet Explorer
- Protección de WIFI
- Uso correcto y configuración del correo electrónico
- Conocimiento de aspectos legales en lo que respecta a privacidad en el internet.

Para que el personal empiece a tomar conciencia en el tema de gestión de seguridad el directorio además de lo ya mencionado deberá aplicar otras estrategias como clips de vídeo, ilustraciones, posters, salvapantallas.

La formación para promover la concientización tiene como objetivo permitir que el personal reconozca los problemas e incidentes de seguridad de la información y respondan de acuerdo con las necesidades de su función de trabajo.

5.8.2.3.- Procedimiento disciplinario

Actualmente es de conocimiento de todo el personal cuales son las acciones a tomar si algún empleado viola la seguridad de la información; es necesario que este procedimiento este por escrito, y que todo el personal que trabaje en el complejo FAME, incluso candidatos a puestos y terceros ejecutando tareas pues deberán tener presente este documento en el cual se aclarara cuales serán las consecuencias legales por haber atentado contra la información.

Este procedimiento disciplinario deberá ser totalmente imparcial y para todo el personal, para la toma de decisión se tendrá que tomar en cuenta si fue primera vez o si ha sido reiterativo, el impacto sobre el negocio y los conocimientos informáticos del supuesto agresor antes de que el directorio dicte la sanción respectiva.

5.8.3.- Finalización o cambio del puesto de trabajo

5.8.3.1.- Cese de responsabilidades

El complejo tiene definido las responsabilidades y funciones de cada persona, pero es obligación tener un procedimiento escrito el cual dicte los pasos a seguir cuando se dé el cese de funciones por parte de un empleado.

Es necesario también que en el contrato y acuerdo de confidencialidad se estipule la no divulgación de información por un periodo definido o indefinido después de romper relaciones laborales con el complejo.

Por lo general es el departamento de Recursos Humanos el responsable de cerrar o terminar el proceso y en conjunto con el Departamento de Tecnología e Información harán cumplir todos los procedimientos de seguridad requeridos por la política del complejo.

Si el término de funciones viene dado por personas pertenecientes a terceros, pues sus representantes serán advertidos del cambio y se dará una reunión en la cual se explicara el por qué de la modificación

5.8.3.2.- Restitución de activos

Cuando se da la finalización de relaciones laborales entre un empleado y el complejo FAME, el mismo llena un acta de recepción, en la cual constan todos los activos que se le fueron entregados al comienzo de sus funciones, las cuales fueron respaldadas con un acta de entrega.

Todo dispositivo móvil documentación corporativa y de equipos, equipos informáticos propiamente, software, tarjetas de acceso, tarjetas de crédito si fuese el

caso, deberá ser entregado al personal encargado, los mismos se encargaran de verificar el estado de los activos y proceder con lo estipulado en contrato.

5.8.3.3.- Cancelación de permisos de acceso

Cuando se da el cese de funciones laborales o se producen cambios entre departamentos, pues los encargados de departamento deberán comunicarse con el departamento de Tecnología e Información para modificar los derechos de acceso de un individuo a los activos asociados con los sistemas de información y a los servicios.

Los derechos de acceso deben incluir acceso físico a instalaciones del complejo como oficinas y bodegas y acceso lógico como contraseñas para acceso a información y sistemas

5.9.- SEGURIDAD FÍSICA Y AMBIENTAL

5.9.1.- Áreas seguras

5.9.1.1.- Perímetro de seguridad física

En lo que respecta a perímetros de seguridad física, FAME cuenta con personal de seguridad en la entrada principal al Complejo, filtro por el cual debe pasar cualquier persona que desea entrar a las instalaciones, los mismos deberían escoltar a la persona hasta llegar a las instalaciones deseadas, para que no se pueda dar el hecho de desviarse u ocultarse. De la misma manera el personal de seguridad deberá escoltar hasta la salida a la persona, cuando la misma haya culminado su visita.

Cada edificio o perímetro que conforma el Complejo debe estar claramente identificado, y cada uno deberá tener seguridad independiente, el nivel de la misma dependerá de los activos e información que se encuentren en su interior.

Actualmente las oficinas de Fame, cuentan con entradas físicas como puertas y ventanas, las mismas que tienen una protección externa adicional; pero es necesario recomendar que se haga una mantenimiento de estas seguridades cada seis meses, de lo contrario en caso de intrusión, serán de muy fácil acceso, así como también analizar la opción de implementar doble barrera para que así se va en mayor dificultad el hecho de querer irrumpir en las instalaciones.

El complejo deberá tomar en cuenta el hecho de tener en cada departamento, una recepción en la cual toda persona desconocida deberá permanecer hasta que su contacto se haga presente.

Es muy necesario que el Complejo FAME, presione al Departamento de Seguridad Industrial para que diseñen salidas de emergencia en caso de cualquier tipo de amenaza ya que al momento no se dispone de las mismas; una vez diseñado el directorio deberá aceptar, poner dentro del presupuesto y proceder con la construcción y adecuación de las instalaciones; ya que al momento el personal corre mucho peligro y los mismos desconocen de este riesgo por falta de conocimiento.

Por otro lado, el complejo actualmente posee un sistema de vigilancia electrónica a través de cámaras de seguridad, este sistema deberá ser revisado cada 3 meses para determinar que su funcionamiento sea el correcto y poder mantenerlo sin problemas, se debe tomar en cuenta que toda oficina, pasillo, puerta, ventana, bodega debe ser vigilada por este sistema, así como también el complejo debe tener un sistemas de alarma con sirena y detección de intrusos.

Para lo que respecta a instalaciones donde se da el procesamiento de información o donde se encuentran servidores principales, debe estar aislada de instalaciones ocupadas por terceros; que si bien es cierto tienen firmado contrato, acta de confidencialidad, etc. No se puede confiar los accesos.

Por parte del complejo no se tiene ningún tipo de procedimiento escrito en cuanto a seguridad de instalaciones, por lo cual se deberá tomar muy en cuenta, y el Departamento de Tecnología e Información junto con el Departamento de Seguridad industrial, deberán enfocarse en desarrollar uno adecuado siguiendo estas recomendaciones.

5.9.1.2.- Controles físicos de entrada

Es necesario que tanto el personal de seguridad al exterior del Complejo, como el personal de recepción, registren en bitácora todo acceso de parte por parte visitantes a las instalaciones.

El Complejo Fabril Fame, en cuanto a accesos, no dispone de controles automatizados, por lo cual se debería presentar al directorio esta opción; ya que lo mejor para mantener alejado a intrusos, aparte de seguridades físicas como barreras, alarmas, etc. Es manejarse con tarjetas electrónicas las cuales sean las únicas que permitan abrir puertas.

Toda visita deberá portar una identificación entregada por el personal de Seguridad, que permitirá que la persona sea identificada; de la misma manera el personal del Complejo debería tener restricciones en cuanto a accesos, dependiendo de su cargo y funciones desempeñadas.

5.9.1.3.- Seguridad de oficinas, despachos y recursos

El Departamento de Seguridad Industrial en la actualidad se encuentra desarrollando normas y políticas de seguridad física para el complejo, en estas se recomienda que en cuanto a seguridad en oficinas, las mismas sean resguardadas por personal de vigilancia; que se encuentren alejadas de lugares donde se da el procesamiento de información.

Las edificaciones u oficinas que posean información confidencial del Complejo no deberán tener etiquetas que delaten su objetivo, pero será necesario que tengan las protecciones necesarias.

5.9.1.4.- Protección contra amenazas externas y del entorno

Este punto también es responsabilidad del Departamento de Seguridad Industrial, el mismo mensualmente da charlas al personal acerca de cómo prevenir y como actuar ante alguna amenaza externa como incendios, terremotos, inundaciones, explosiones, goteras, etc.

Todo material inflamable debe estar situado a distancia prudente de las oficinas, de la misma manera la bodega de repuestos debe estar apartada, para que en caso de emergencia o destrucción de instalaciones, los repuestos permanezcan intactos.

En cada instalación del complejo FAME deberá existir equipo contra incendios, y se deberán realizar simulacros de emergencia cada tres meses para que se pueda evaluar el conocimiento del personal para este tipo de casos.

Es importante que el Departamento de Seguridad Industrial en conjunto con el Departamento de Tecnología e Información, realicen o elaboren un análisis de riesgos para poder costear y categorizar equipos textiles, equipos informáticos, etc.

5.9.1.5.- El trabajo en áreas seguras

Para realizar trabajos en áreas seguras es necesario que el personal trabaje en ellas bajo custodia, y solo si es que existe la necesidad.

Es recomendable que ningún trabajo en áreas seguras se realice sin ningún tipo de supervisión, es decir siempre debería existir la persona que realice las tareas junto con personal de vigilancia o personal superior.

Se debe prohibir el acceso con cualquier tipo de dispositivo fotográfico, de audio o video; ya que como política es necesario que ningún tipo de información salga del Complejo.

5.9.1.6.- Áreas aisladas de carga y descarga

Como procedimiento, el Complejo tiene dispuesto que cuando se haga un despacho o recepción de carga, se realice la actividad en partes externas a las edificaciones, sin necesidad de que el personal ajeno ingrese a oficinas, bodegas, etc.

Personal del complejo es el encargado de recibir la carga y llevarla a su lugar, así mismo ayudan con el despacho de lo pedido.

Es importante que en este procedimiento se tome en cuenta el hecho de inspeccionar detenidamente la carga que llega a la Organización para determinar

posibles amenazas o descartar las mismas; y todo ingreso o salida de material deberá ser registrado en bitácora, además de que todo ingreso deberá ser tratado según el control de Gestión de Activos.

5.9.2.- Seguridad de los equipos

5.9.2.1.- Instalación y protección de equipos

Para la protección de los equipos en contra de las amenazas del entorno y el acceso no autorizado se deberán tomar en cuenta los siguientes parámetros:

- El equipo deberá estar ubicado de manera que se minimice el acceso innecesario a las áreas de trabajo.
- Los medios de procesamiento de la información que manejan datos confidenciales deberán ubicarse de manera que se restrinja el ángulo de visión para reducir el riesgo que la información sea vista por personas no autorizadas durante su uso; y se deberán asegurar los medios de almacenaje para evitar el acceso no autorizado.
- Se deberán aislar los ítems que requieren protección especial para reducir el nivel general de la protección requerida.
- Se deberá prohibir comer, beber y fumar en la proximidad de los medios de procesamiento de información.
- Se deberán monitorear las condiciones ambientales; tales como temperatura y humedad, que pudiera afectar adversamente la operación de los medios de procesamiento de la información.

- Se deberá aplicar protección contra rayos a todos los edificios y se debieran adaptar filtros de protección contra rayos a todas las líneas de ingreso de energía y comunicaciones.

Estas actividades deberán ser planificadas por el Departamento de Tecnología e Información y puestas en marcha al momento de la instalación de los equipos.

5.9.2.2.- Suministro eléctrico

Todos los suministros, no solo eléctrico sino también agua, alcantarillado, calefacción, aire acondicionado, etc. Deberán ser inspeccionados en una primera etapa para determinar si cumplen con su objetivo y seguido se les dará mantenimiento periódico trimestral.

Dentro de las tareas del complejo estarán la elaboración de simulacros en los cuales se pondrá en funcionamiento estos suministros para garantizar su funcionamiento adecuado y minimizar los riesgos debido a posibles fallas.

Por otro lado haciendo referencie al suministro eléctrico, el complejo FAME actualmente posee un generador por cada edificio, mas no en el nuevo edificio administrativo; esto deberá ser temporal y se deberá obligatoriamente montar un generador que de soporte a toda la edificación, en cuanto a combustible para los generadores se debe realizar un chequeo diario para tener un total abastecimiento.

Se dispone de UPS centralizado para los equipos y edificaciones cercanas, para sectores alejados como en bodegas, etc. Se tiene un ups por cada equipo; todas estas fuentes de suministro eléctrico deberán ser revisadas mensualmente y poder recargar o cambiar baterías.

En cuanto a iluminación de las edificaciones se refiere, es necesario que se tome en cuenta el establecer una segunda fuente de energía, para que en caso de emergencia o falla en el suministro principal de electricidad; entre en labor sin hacer uso del generador.

5.9.2.3.- Seguridad del cableado

Es importante que el Departamento de Seguridad Industrial en conjunto con el Departamento de Tecnología e Información, formen un esquema de protección del cableado eléctrico y de comunicaciones de todo el Complejo, para proteger contra posibles interceptaciones o daños.

El personal que trabaja en el Complejo ha tratado de mejorar sus instalaciones pero se ha dejado de lado puntos sumamente importantes, los cuales ponen en riesgo a toda su infraestructura, si hablamos del cableado, consideraremos:

- Tanto el cableado eléctrico como el cableado de comunicaciones debería ser subterráneo y de difícil acceso.
- Los puntos terminales eléctricos y de comunicaciones deberían tener una caja de protección con cerradura.
- El cableado eléctrico como de comunicaciones deberían ser blindados y estar separados para evitar interferencias.
- Tener siempre a mano los planos donde se tenga identificado todo el cableado del Complejo.
- Revisión mensual de todo el cableado para descartar que exista cualquier tipo de dispositivo conectado no autorizado.

5.9.2.4.- Mantenimiento de equipos.

En cuanto a mantenimiento de equipos; el Complejo FAME dispone de contrato con la empresa AKROS, quienes son los encargados de dar el mantenimiento preventivo y correctivo.

El personal del Departamento de Tecnología e Información se encargara de dar seguimiento al mantenimiento que se dé a los equipos por parte de la empresa contratada para determinar que sea el adecuado. Además de conservar una bitácora en la cual se detalle:

- Fecha de revisión del equipo
- Área a la cual pertenece el equipo.
- Nombre de la persona que reporta la falla.
- Descripción del error del problema.
- Responsable de solucionar el problema.
- Descripción de la respuesta inicial ante el problema.
- Descripción de la solución al problema.
- Fecha en la que se soluciono el problema.

5.9.2.5.- Seguridad de los equipos fuera de las instalaciones

Es recomendación que por parte del directorio se permita al personal a trabajar fuera de oficinas llevando consigo equipos pertenecientes al Complejo.

Previo a la autorización se debe tomar en cuenta:

- Tener un seguro sobre todos los equipos de procesamiento de información.

- Se debe instalar en todo equipo un software de conexión remota para poder tener comunicación con el sistema de archivos del Complejo.
- Se debe capacitar al personal para que conozcan de los riesgos de los equipos cuando están expuestos al exterior.
- Todo equipo que salga de las instalaciones del Complejo deberá ser registrado en bitácora.
- El personal que maneje el equipo será el responsable de mantener el equipo sin daños.

5.9.2.6.- Seguridad en la reutilización o eliminación de equipos

Sera decisión del Departamento de Tecnología e Información específicamente del personal encargado de equipos en conjunto con la persona designada por el director del departamento, quienes dicten mediante un informe, si un equipo estará en condiciones de reutilizarse o si tendrá que ser destruido físicamente.

En caso de ser reutilizado, la información que haya residido en el equipo, tendrá que ser eliminada o sobrescrita para que no pueda ser recuperada por otra persona.

5.9.2.7.- Traslado de activos

Por política ningún equipo, o información debería ser llevado a las fueras del Complejo sin previa autorización.

Todo equipo que salga o ingrese pues deberá ser registrado en bitácora y se deberá implementar límites de tiempo en cuanto a retiro de los equipos, de la misma

manera será necesario dar seguimiento para verificar el cumplimiento de las políticas.

5.10.- GESTIÓN DE COMUNICACIONES Y OPERACIONES

5.10.1.- Responsabilidad y Procedimientos de Operación

En base a la norma ISO 27002, y al plan de seguridad, se deberá definir claramente el alcance de cada departamento y a su vez segregar las tareas, cuando así se requiera para bajar el riesgo por negligencia o mal uso deliberado.

La documentación de procedimientos, directrices de seguridad, desde la física, hasta la seguridad de IT, deberá estar definida y se usará de manera sistemática, definiendo los roles y responsabilidad y utilizando los formularios definidos.

Como parte de la operación se debe tener en cuenta la métrica de los procesos, tomando en cuenta los tiempos relativos al manejo de la Información e Informática, tales como por ejemplo los tiempo de implementación de ajustes a los sistemas, tiempos sin la herramienta, esto permite tomar el control en los momentos de crisis.

La documentación de los procedimientos de operación, su publicación y disponibilidad para todos los usuarios se debe garantizar, manteniendo estos como política de la organización.

Todos los cambios en los sistemas, en los recursos de tratamiento de la información, en los equipos, se deben mantener en planillas, guías y modelos para la gestión de la operación, utilizando de ser posible herramientas de distribución de paquetes, tales como Enteo NetInstall, Altiris, Microsoft System Center Configuration Manager.

Una de las tareas a realizarse de manera periódica, es la toma de inventario tanto del Software como del Hardware.

Para poder mantener las responsabilidades definidas, se debe segregar las tareas a cada área, y dentro de la misma asignarla a una persona o equipo de trabajo, con el fin de reducir las oportunidades de un proceso no autorizado o uso indebido o intencionado tanto de activos de la organización, utilizando planillas, guías y modelos definidos para cada efecto.

Separación de los recursos para desarrollo y producción, así como para pruebas, es importante para reducir los riesgos de un acceso no autorizado o de cambios al sistema operacional.

5.10.2.- Gestión de la provisión de servicios por terceros

Para lograr el que servicio contratado a terceros se cumpla de acuerdo a los procedimientos y procesos internos es indispensable la supervisión, esta se debe realizar y mantener durante todo el proceso de servicio.

Mantener e Implementar el nivel de seguridad apropiado, para el control de la prestación de servicios de terceros.

Se debe verificar la implementación de acuerdos, monitorear el cumplimiento de cambios para asegurar que los servicios cumplan con todos los requerimientos acordados con terceros.

¿El valor que se paga por el servicio, es lo que se recibe?

Responder esta pregunta tiene que respaldar con hechos, supervisando al equipo de terceros y sus servicios, revisando periódicamente los niveles de

cumplimiento, comparando con los registros de supervisión, siempre fijándose en la seguridad de la información, empezando por la seguridad física.

Siempre se debe medir los tiempos de inactividad, por incumplimiento, Evaluar rendimientos, calidad, entrega, costos.

Se debe garantizar los controles de seguridad, definir servicio y niveles de entrega incluidos en el acuerdo de entrega de servicio externo sean implementados, operados y mantenidos por la parte externa.

5.10.3.- Planificación y Aceptación del Sistema

El objetivo de la planificación, es minimizar los riesgos y fallas en los sistemas, así como evitar la pérdida de la información, por lo que se requiere preparar a detalle el proceso de aceptación de los sistemas, para que la afectación sea mínima y los recursos sean los adecuados.

Adicionalmente se requiere realizar proyecciones para de esta manera dimensionar el crecimiento y reducir la futura saturación de los sistemas.

Todos los requisitos para los sistemas nuevos se deben documentar, de manera que se apruebe la aceptación de cada uno.

Los procedimientos operativos se utilizaran en el día a día del mantenimiento o cambio en los sistemas y la infraestructura con el fin de garantizar el mejor servicio posible. Estos procedimientos deben estar documentados en un nivel adecuado de detalle para que el equipo del departamento los utilice cuando así se requiera.

5.10.4.- Protección contra Códigos Malicioso y Descargable

Es indispensable adoptar las medidas apropiadas para proteger a los sistemas y la información de cualquier código malicioso, como por ejemplo virus, gusanos de red, códigos troyanos, que puedan afectar a los servidores y los equipos de todos los usuarios.

Todo el personal es responsable de asegurarse de no introducir ninguno de los elementos señalados, siguiendo las políticas de software.

Se recomienda considerar las siguientes directrices

- Establecer una política formal que prohíba el uso de software no licenciado y no probado, sea descargado a través de redes externes o cualquier otro medio
- Llevar a cabo revisiones regulares del software y del contenido de datos de los sistemas que dan soporte a los procesos críticos del negocio.
- Instalación y actualización regular del software de detección y reparación de códigos maliciosos para explorar los computadores y los medios, como control preventivo o de forma rutinaria.

5.10.5.- Copias de Seguridad

Para garantizar la disponibilidad continua de la información y la recuperación ante un desastre, se deben establecer procedimientos automáticos de respaldo de la información, adicionales a los de cada sistema deberá mantener.

La política de respaldos debe mantener toda la documentación necesaria para realizar la recuperación, con procedimientos escritos y de fácil acceso.

Se debe mantener una política programada de respaldo de manera diaria, semanal, mensual y anual y proteger dichos respaldos fuera de las instalaciones de la organización, con control de acceso a los mismos.

5.10.6.- Gestión de Seguridad de RED

Las conexiones a infraestructura de red física como inalámbrica debe realizarse de una manera controlada, la gestión de la red es fundamental y se deben aplicar los siguientes controles.

- Tiene que haber responsabilidades y procedimientos claros para la gestión de equipos remotos y usuarios
- Se deben definir políticas de trabajo remoto y políticas de manejo de medios magnéticos extraíbles.
- La responsabilidad operativa de las redes, cuando sea posible, debe estar separado de operaciones de los computadores.
- Deben establecerse controles y protección para los datos que pasan por la red, realizando procesos de cifrado o utilizando herramientas para tal propósito.

La arquitectura de red debe estar documentada y almacenada con parámetros de configuración de todos los componentes de hardware y software que componen la misma, sobre todo cuando se usa equipos activos administrables.

Se debe mantener respaldos de la configuración de todos los equipos de red.

Todos los componentes de la red deben registrarse como activo. Todos los equipos deben mantener configuración de seguridad alta, a un nivel apropiado para permitir el trabajo transparente para los usuarios autorizados.

Se debe configurar los sistemas operativos, de manera que no se permita a los usuarios realizar cambio alguno en la configuración de los elementos de red.

5.10.7.- Manejo de los Medios Magnéticos y de Información

El manejo de medios e intercambio, debe estar controlado y de acuerdo a las políticas establecidas para el efecto, los elementos de hardware externos como memorias, discos, cds, dvds, etc., deben manejarse por personal definido como responsable para tal efecto.

Toda operación con elementos ajenos a la organización, están restringidos, y no pueden utilizarse dentro de las instalaciones de la empresa.

5.10.8.- Intercambio de Información

Para realizar intercambio de información se deben cumplir con las reglas establecidas por la organización, y utilizando únicamente los medios definidos para tal efecto.

Tomando en cuenta que la organización tiene definido y cuenta con todos los procedimientos de seguridad de la red, se recomienda para este proceso, el uso de la misma, de manera que se comparta cualquier información por la red de la organización y se evite, mientras sea posible, el uso de equipos externos o móviles.

5.10.9.- Servicios de correo electrónico

Tomando en cuenta que este medio es uno de los más utilizados para compartir información, se debe definir las políticas de seguridad adecuadas para el uso de la misma.

Es el Correo Electrónico el medio más rápido para realizar cualquier tipo de comunicación, tanto interna como externa, por lo que se debe realizar el seguimiento de todo el tráfico, sin manipular o revisar su contenido, pero manteniendo todo el control para evitar problemas tanto de pérdida o salida de información, como de entrada de códigos maliciosos.

De ser factible, las herramientas y sistemas utilizados, deberán contemplar el uso automatizado de esta herramienta, de manera que su uso sea mucho más generalizado.

5.10.10.- Monitoreo

Si los sistemas permiten, el monitoreo se debe realizar de manera automatizada, de tal forma que se mantenga un registro (log) de actividad de cada proceso o elementos, tanto de hardware o software.

Cuando no se disponga de dichas herramientas, el monitoreo de toda actividad relacionada se debe realizar por el personal definido para el efecto y de manera sistemática.

Se deben revisar de manera periódica toda la funcionalidad de las herramientas y equipos de seguridad, desde la física hasta la de la información.

5.11.- CONTROL DE ACCESOS

5.11.1.- Requisitos de negocio para el control de accesos

El control de acceso puede ser algo muy sencillo, desde una llave hasta el uso de una tarjeta electrónica para bloquear y desbloquear una puerta. Esta función, sigue siendo una de las más importantes y básicas.

En la mayoría de los casos, se limita la entrada y salida durante determinadas horas, permitiendo que todo el personal tenga la llave, sin correr el riesgo de que alguien no autorizado acceda a las instalaciones fuera del horario normal.

Adicionalmente existe el control, la comprobación y el reporte de las personas que intenten entrar, la hora de en la que sucede y su registro.

Por otro lado, un sistema de control de accesos puede ser la mejor de las alternativas, para evitar cualquier problema, confirmando de esta manera que la seguridad se inicia por la parte física, el sistema debe ser integrado y con registros de accesos, de manera que convierta a toda la empresa en un sistema de esclusas, tenga gestión integrada de video vigilancia, control de visitantes, administración de iluminación, alarmas contra incendio, entre otras.

Las soluciones actuales están ligadas de manera directa con los sistemas informáticos (IT), lo que se denomina “Convergencia Física y Lógica”, para reducir el riesgo de accesos no autorizados a la empresa y sus plataformas de información y sistemas.

5.11.2.- Gestión de acceso de usuario

Definiendo los requisitos tenemos que incluir todo el control de acceso, desde el físico hasta el lógico, de manera que se maneje un solo sistema de identificación del personal, así como de las visitas y personal de terceros.

Se deberá concientizar a los ejecutivos, empleados, personal de terceros, en fin a todos los usuarios sobre sus responsabilidades por el mantenimiento de controles de acceso, en particular todos aquellos relacionados con el uso de contraseñas y seguridad del equipo de trabajo.

Es deseable mantener una política de escritorio y pantalla despejados para reducir el riesgo de acceso no autorizado o daño de reportes, medios y servicios de procesamiento de Información.

5.11.3.- Responsabilidades del usuario

Es responsabilidad de cada ejecutivo, empleado, personal de servicios de terceros y visitante, mantener su identificación de manera que se distinga la autorización que tiene para estar en cada lugar de la planta u oficinas.

Con este procedimiento se evita el acceso de usuarios no autorizados, el robo y riesgos de pérdida de la información o de los servicios y equipos de procesamiento de la misma.

La cooperación de cada uno de los usuarios autorizados es esencial para la eficacia del control de accesos.

Una vez cubierto el área física, los usuarios son responsables de cada una de las claves de acceso, tanto a los servidores como a cualquier equipo informático al que estén autorizados.

Si se encuentran utilizando recursos de red, deberán cumplir con los mismos esquemas de seguridad que están definidos para el accesos local, es decir si están trabajando en equipos móviles o desde sus hogares, el sistema de control de acceso deberá controlar todos estas alternativas y garantizar los accesos.

La gestión de claves de acceso deberá cumplir con todas las reglas de seguridad, y se deben actualizar en un plazo no mayor a 65 días, y en caso de tratar de ingresar a los sistemas por más de 3 veces, el sistema deberá bloquear dicha clave y el usuario tendrá que actualizar sus claves de acceso.

Definidas las claves de acceso, es indispensable que se mantenga un registro de los permisos y privilegios que cada usuario y clave mantienen.

Las definiciones de accesos y privilegios, deberán ser revisadas periódicamente, para garantizar que no se tenga riesgos o perdida de información o similares.

5.11.3.- Control de acceso al sistema operativo y Control de acceso en red

Tomando en cuenta que hoy en día se cuenta con todas las herramientas de automatización, se deberá limitar el acceso en todos los equipos al sistema operativo, usando herramientas para que el usuario, disponga de todo aquello que es indispensable para su trabajo eficiente, pero que no tenga acceso a los sistemas operativos, pues estos son altamente vulnerables a ataques de todo tipo.

El control de acceso de este tipo debe manejar procedimientos seguros de inicio de sesión en la red y en los equipos de manera local, identificando y autentificando a cada usuario, manteniendo logs de actividad de inicio y de fin de sección.

El sistema de autentificación debe disponer de una herramienta de administración de usuarios y contraseñas, que permita fijar normas de seguridad de nivel alto, para evitar posibles problemas de accesos no autorizados.

Las claves de acceso de cada usuario debe tener por lo menos 7 caracteres, entre letras y números, ningún equipo debe mantener usuarios locales para acceso sin clave, o con similares al usuario.

El uso de recursos de la red, debe estar definido para cada usuario, todos los accesos a impresoras, recursos compartidos y demás, deben estar definido para cada nivel de acceso y para cada grupo o usuarios.

Para los casos en que los usuarios dejan sus equipos sin actividad alguna, se debe controlar que el sistema realice una desconexión segura en no más de 4 minutos.

5.11.4.- Control de acceso a las aplicaciones

El control de accesos de las aplicaciones, debe ser un paso adicional, y por seguridad no debe estar integrado con el sistema operativo, cuando sea posible deberá tener un registro de auditoría de accesos.

Las aplicaciones que mantengan información sensible, debe tener controles adicionales, y niveles de autorización para su acceso.

Los registros de auditoría deben ser conservados por un mínimo de seis meses, registrando las excepciones y otros eventos relacionados con la seguridad.

Como mínimo, el registro de auditoría de accesos deberá contener la siguiente información:

- Identidad del sistema.
- ID de usuario.
- Inicio de sesión con éxito y sin éxito.
- Cierre de sesión con éxito y sin éxito.
- Acceso a las aplicaciones no autorizadas.
- Cambios en las configuraciones del sistema.
- Uso de cuentas privilegiadas (por ejemplo, gestión de cuentas, los cambios de políticas, configuración de dispositivos).

Las aplicaciones con información sensible deben tener un control definido y limitado de usuarios.

Los registros de auditoría deben ser protegidos de accesos no autorizados que podrían resultar en modificaciones de la información registrada o que sea eliminada. El administrador de sistemas debe evitar el borrado o la desactivación de los registros de su propia actividad.

Para el caso de datos sensibles (clasificados), estos deben ser almacenados por separado. Los datos enviados o recibidos deben mantenerse separados de los datos no clasificados. El personal puede hacer esto utilizando unidades especiales de la red.

5.11.5.- Informática móvil y tele trabajo

Las herramientas como Laptops, Note Books, I-Pads, Net Books, deben estar registradas en el sistema de activos y con un control de uso que mantenga controles de acceso, uso, entrada y salida.

Para el caso de trabajo fuera de las instalaciones, se debe mantener equipos específicos, de manera que ninguna información normal o sensible pueda salir de las instalaciones.

Cuando sea necesario en la organización utilizar dispositivos de computación móvil, se debe asegurar que la información no se vea comprometida, se debe establecer una política que incluya los riesgos de trabajar con este tipo de equipos, especialmente en áreas sin seguridad y protección.

En áreas públicas fuera de la seguridad de la organización, se debe tener especial cuidado cuando se utilicen equipos y dispositivos móviles, se deben instalar en estos dispositivos una protección adecuada para evitar el acceso no autorizado o la divulgación de la información almacenada y procesada por éstos.

Los dispositivos de computación móvil deben estar protegidos físicamente contra robo.

Cuando se requiera trabajar de manera remota para la Organización, es decir, fuera de las instalaciones, se debe proteger adecuadamente el lugar de trabajo remoto contra: robo del equipo o información, distribución no autorizada de información, accesos remotos no autorizados a los sistemas internos o mal uso de dispositivos.

Se deben implementar controles y planes operativos para las actividades de trabajo remoto para mantener registros de accesos y conexiones al centro de cómputo principal.

Se recomienda tener en cuenta los siguientes controles:

- Seguridad física.
- Dotación del equipo o mobiliario adecuados para las actividades de trabajo remoto.
- Definición del trabajo permitido y horas de trabajo.
- Clasificación de la información que puede ser utilizada.
- Sistemas y servicios internos a ser accesados.
- Suministro de equipo de comunicación adecuado.
- Soporte y mantenimiento para hardware y software.
- Auditoría, seguimiento y respaldos de seguridad de la información.

5.12.- ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

5.12.1.- Requisitos de seguridad de los sistemas

5.12.1.1.- Análisis y especificación de los requisitos de seguridad

Es necesario que personal designado de cada área, por el hecho de ser conocedores en su materia, aporten con ideas en cuanto a requisitos de control o seguridad se refiere, para que sean tomados en cuenta tanto en escenarios de

cambios a los sistemas de información actuales o nuevos paquetes de software que vayan a ser incorporados.

Estos controles deberían reflejar el valor para el negocio de los activos de información que están involucrados; así como los riesgos a presentarse debido a la falta de los mismos.

Los requisitos de seguridad siempre deben ser tomados en cuenta al inicio de cualquier proyecto de desarrollo de aplicaciones informáticas o adquisición de las mismas debido a los costos de implementación son menores cuando se está en etapa de diseño de la herramienta.

5.12.2.- Seguridad de las aplicaciones del sistema

5.12.2.1.- Validación de los datos de entrada

Se deberá contar con personal que se dedique a realizar Test de calidad de los sistemas de información, el mismo deberá asegurarse que todas las entradas en los aplicativos, tengan validaciones adecuadas, tanto en los módulos de transacciones como en los de mantenimiento. Algunos controles importantes a considerarse son:

- Valores fuera de rango.
- Caracteres inválidos en campos de datos.
- Datos faltantes o incompletos.
- Volúmenes de datos que exceden los limites inferior y superior.
- Controles de datos no autorizados o inconsistentes.
- Revisión periódica de los contenidos de campos clave o archivos de datos para confirmar su validez e integridad.

- Inspección de los documentos de entrada para detectar cambios no autorizados en los datos de entrada.
- Procedimientos para responder a errores de validación.
- Procedimientos para determinar la verosimilitud de los datos.
- Determinación de las responsabilidades de todo el personal involucrado en el proceso de entrada de datos.

5.12.2.2.- Control del proceso interno

Se deberán incorporar procedimientos de verificación de validación en las aplicaciones para poder detectar cualquier posible corrupción en la información.

En la etapa de diseño se deberá garantizar que se minimicen los riesgos de falla en el procesamiento, ya que esto repercute en la integridad del sistema y muy posiblemente en la información.

- Algunos puntos a considerarse son:
- Funcionalidad en cuanto a Agregar, Modificar o Borrar
- Procedimientos para evitar que los programas se ejecuten en orden erróneo
- Protección contra ataques empleando desbordamiento / exceso en el búfer
- Verificaciones de la integridad y la autenticidad

El Administrador de Sistemas de Información deberá preparar una lista de chequeo apropiada, y deberá documentar las actividades, y los resultados deberán mantenerse seguros.

5.12.2.3.- Autenticación de mensajes

Dentro de los controles requeridos, es necesario también analizar los riesgos a los que están expuestos los mensajes que interiormente los aplicativos manejan, por lo cual es necesario se realice una evaluación para determinar si se requiere o no integridad dentro del mismo y que controles se pueden incorporar.

5.12.2.4.- Validación de los datos de salida

En la etapa de diseño el personal designado por la Administración del Departamento de Tecnología e Información, deberá realizar una validación a todas las posibles salidas que el sistema posea para validar que todo el procesamiento y almacenamiento de información es correcto. Este sondeo deberá incluir:

- Probar si los datos de salida son razonables.
- Suministro de información suficiente para que un sistema de procesamiento posterior determine la exactitud, totalidad, precisión y clasificación de la información.
- Procedimientos para responder las pruebas de validación de salidas

Generalmente los sistemas pasan por etapa de prueba en cuanto a entradas y mensaje, dejando a un lado el control de las salidas debido a que se asume que si lo anterior es correcto entonces el resultado es correcto pero ha pasado que esta suposición no siempre es válida; es decir, los sistemas que se han sometido a prueba aún pueden producir salidas incorrectas en algunas circunstancias.

5.12.3.- Controles criptográficos

5.12.3.1.- Política de uso de los controles criptográficos

El Director del Departamento de Tecnología e Información, junto con el directorio del complejo FAME, deberán estudiar la opción de implementar una política criptográfica, que permita dar seguridad a toda la información de la empresa. En esta política se deberá tomar en cuenta lo siguiente:

- Los principios bajo los cuales se necesitaría proteger la información.
- El uso de encriptación para proteger medios móviles o extraíbles.
- Recuperación de información encriptada en caso de pérdida o amenazas a las claves
- Normas que se han de adoptar para la implementación eficaz en toda la organización
- Impacto de la utilización de información encriptada

El uso de una política criptográfica, ayudara de manera sustancial al complejo en cuanto a confidencialidad, autenticidad y no–repudio de la información se refiere.

5.12.3.2.- Cifrado

Si una política criptográfica es implementada, pues será necesario que se gestionen procedimientos los cuales contemplen:

- Protección de claves contra modificación, pérdida y destrucción.
- No divulgación de claves privadas
- Generación de distintas claves para cada aplicativo

- Cambio y actualización de claves
- Revocación de claves
- Recuperación de claves corruptas

Para reducir la probabilidad de poner en peligro, activar o desactivar se deberían definir fechas para las claves de modo que sólo se puedan utilizar durante un periodo de tiempo limitado.

5.12.4.- Seguridad de los ficheros del sistema

5.12.4.1.- Control del software en explotación

El Administrador del Departamento de Tecnología e Información deberá establecer un procedimiento el cual encamine al personal del área a mantener de manera organizada y correcta los sistemas en producción, para esto se deberá tomar en cuenta:

- Cualquier tipo de actualización a los aplicativos informáticos, deberán ser realizadas por personal designado, debidamente capacitado y únicamente después de tener la autorización de su director.
- Los Sistemas operativos deberán contener códigos ejecutables más no en desarrollo.
- Todo software deberá ser instalado únicamente después de haber realizado pruebas exhaustivas y que las mismas sean 100% satisfactorias.

- Cualquier tipo de pruebas aplicadas a los aplicativos deberán ser realizadas en escenarios que no tengan ningún tipo de contacto con el ambiente de producción.
- Todo sistema instalado deberá tener su documentación respectiva, la misma que deberá ser almacenada en lugares seguros con acceso autorizado.
- Se debe tener políticas de restauración a puntos anteriores a los cambios por cualquier tipo de problema
- Es necesario llevar una bitácora la misma que contenga todos los cambios y actualizaciones realizadas de cada equipo
- El software suministrado por el vendedor utilizado en los sistemas operativos se debería mantener en el nivel con soporte del proveedor.
- En toda decisión para mejorar a una nueva versión se debería contar con los requisitos del negocio para el cambio, y la seguridad de la nueva versión, es decir, la introducción de nueva funcionalidad en el sistema o la cantidad y gravedad de los problemas de seguridad que afectan a esta versión.
- Los parches de software se deberían aplicar cuando pueden ayudar a eliminar o reducir las debilidades de la seguridad.
- El acceso físico o lógico únicamente se debería dar a los proveedores para propósitos de soporte, cuando sea necesario, y con aprobación de la dirección.

5.12.4.2.- Protección de los datos de prueba del sistema

Para escenarios de pruebas, es recomendable que la o las personas encargadas de los sistemas de información pidan que no se utilice Bases de datos que se encuentren en producción, y si por funcionalidad y eficacia de pruebas se debe manejar información personal actual, pues será necesario que antes de empezar, se elimine la configuración de la Base de datos y si es posible eliminar la información transaccional.

En toda etapa de pruebas, para tener un 90 o 100% de certeza en los resultados, es necesario que los datos ingresados sean muy parecidos a los datos reales con los que trabaja el complejo, es por esto que como cierre del ciclo de pruebas, se deberá proceder con la eliminación de la información ingresada; además durante toda la tarea el personal a cargo deberá siempre estar en continuo seguimiento para así evitar fuga de información.

5.12.4.3.- Control de acceso a la librería de programas fuente

En el caso particular del complejo FAME, los códigos fuentes no se encuentran localmente, ya que todos sus sistemas son externos, es decir arriendo o compra de licencias; además de que el complejo no dispone de un área de desarrollo dentro del Departamento de Tecnología e Información pero de igual manera en caso de que el complejo formara un equipo de desarrollo, a fin de reducir la probabilidad de alteración de programas o sistemas, el Administrador de Software deberá mantener un control estricto del acceso a las bibliotecas de programas fuente, según los siguientes puntos:

- Las bibliotecas de programas fuente no deberán ser almacenadas en los sistemas que estén operativos.
- El personal de soporte no debería tener acceso a las bibliotecas de programas fuente a menos que el mismo sea autorizado.
- La actualización de bibliotecas de programas fuente y la distribución de programas fuente a los programadores, solo deberá ser llevada a cabo por el Administrador de Software.
- Los listados de programas deberán ser almacenados en un ambiente seguro.
- El Administrador de Software deberá mantener un registro de auditoría de todos los accesos a las bibliotecas de programas fuente.
- Las viejas versiones de los programas fuente deberán ser archivadas con una clara indicación de las fechas y horas precisas en las cuales estaban en operación, junto con todo el software de soporte, el control de tareas, las definiciones de datos y los procedimientos.
- El mantenimiento y la copia de las bibliotecas de programas fuente deberán estar sujetas a procedimientos estrictos de control de cambios.

5.12.5.- Seguridad en los procesos de desarrollo y soporte

5.12.5.1.- Procedimientos de control de cambios

Es primordial establecer procedimientos de control de cambios, al momento se dispone de bitácoras las cuales almacenan información de todas las actualizaciones modificaciones o cambios realizados, pero en realidad debe existir un procedimiento

amplio el cual indique todo lo necesario para que el control de cambios sea adecuado

Siempre que resulte factible, los procedimientos de control de cambios operativos y de aplicaciones deberán estar integrados. Estos procesos deberán incluir:

- Mantener un registro de los niveles de autorización acordados.
- Garantizar que los cambios son propuestos por usuarios autorizados.
- Revisar los controles y los procedimientos de integridad para garantizar que no serán comprometidos por los cambios.
- Identificar todo el software, la información, las entidades de bases de datos y el hardware que requieran correcciones.
- Obtener aprobación formal del jefe del Departamento de Tecnología e Información y de la dirección para las propuestas detalladas antes de que comiencen las tareas.
- Garantizar que el usuario autorizado acepte los cambios antes de cualquier implementación.
- Garantizar que la implementación se lleve a cabo minimizando la discontinuidad de las actividades de la institución.
- Garantizar que la documentación del sistema será actualizada cada vez que se completa un cambio y se archiva o elimina la documentación vieja.
- Mantener un control de versiones para todas las actualizaciones de software.
- Mantener una pista de auditoría de todas las solicitudes de cambios.

- Garantizar que la documentación operativa y los procedimientos de usuarios se modifiquen según las necesidades de adecuación.
- Garantizar que la implementación de cambios tenga lugar en el momento adecuado y no altere los procesos comerciales involucrados.

5.12.5.2.- Revisión técnica de los cambios en el sistema operativo

Es una tarea básica que debe ser tomada en cuenta en los procedimientos de control de modificaciones y que debe realizarse una vez que los cambios a los sistemas se han elaborado y se han implementado.

El personal encargado deberá monitorear las vulnerabilidades de los sistemas una vez que están en producción, hay que recordar que las actualizaciones de los sistemas operativos (SO) siempre traen consigo cambios a las librerías y registro, lo cual puede ocasionar que los aplicativos sufran inconvenientes debido a que muchos de ellos ocupan archivos del SO.

Este punto conviene ser tomado en cuenta dentro del plan de contingencia y constantemente actualizado. La persona encargada o nombrada por el director del Departamento de Tecnología e Información debe garantizar que la implementación sea transparente y comunicar de manera oportuna de cualquier posible riesgo a su superior.

5.12.5.3.- Restricciones en los cambios a los paquetes de software

Los paquetes de software deberían ser implementados tal como el proveedor los entrega, debido al costo de mantenimiento que se presenta cuando se piden personalizaciones.

El directorio del complejo debe tener en cuenta que los cambios a medida de un aplicativo tienen un costo superior tanto en mantenimiento como en soporte.

Todos los cambios se deberían probar y documentar en su totalidad de manera que se puedan volver a aplicar, si es necesario, para mejoras futuras del software. Si así se requiere, las modificaciones se deberían probar y validar por un organismo de evaluación independiente.

5.12.5.4.- Fuga de Información

Es necesario que los encargados del Departamento de Tecnología e Información tomen en consideración canales que no siempre son visibles, los cuales permiten que exista fuga de información; generalmente estos canales son creados por códigos troyanos.

Para esto es necesario que exista en el debido control en cuanto a instalación de aplicaciones por parte los usuarios, así como la adquisición de sistemas totalmente licenciados, ya que es la única manera de tener garantía ante cualquier suceso.

Además, la persona encargada de los Aplicativos, deberá ser totalmente confiable en cuanto a conocimientos como a integridad. Para así evitar que la fuga de información sea planificada.

5.12.5.5.- Desarrollo externalizado del software

Este punto es muy importante para el Departamento de Tecnología e Información, debido a que el Complejo no posee un departamento de desarrollo, y por lo tanto todos los sistemas que actualmente se encuentran instalados tienen un

proveedor, y antes esto se deben tener en cuenta algunos puntos para así asegurar que los aplicativos son desarrollados acorde a los requerimientos y no presentan ningún inconveniente o riesgo.

Dentro de los puntos a ser considerados:

- Acuerdos de licencias, propiedad de códigos y derechos de propiedad intelectual.
- Certificación de la calidad y precisión del trabajo llevado a cabo.
- Acuerdos de custodia en caso de quiebra de la tercera parte.
- Derechos de acceso a una auditoria de la calidad y precisión del trabajo realizado.
- Requerimientos contractuales con respecto a la calidad del código.
- Realización de pruebas previas a la instalación para detectar códigos troyanos

5.12.6.- Gestión de las vulnerabilidades técnicas

5.12.6.1.- Control de las vulnerabilidades técnicas

Para mantener un control de vulnerabilidades técnicas, es necesario que se disponga de un inventario actualizado de lo que actualmente el Complejo tiene implementado tanto de Software como de Hardware, así como de sus responsables; para con esto realizar el análisis respectivo e identificar dichas vulnerabilidades.

El Director del Departamento de Tecnología e Información, dependiendo de los análisis realizados deberá tomar la acción apropiada y oportuna en respuesta a la

identificación de vulnerabilidades técnicas. Algunos puntos a considerarse para identificar estas vulnerabilidades son:

- El Jefe del Departamento de Tecnología e Información deberá definir y establecer los roles y responsabilidades asociadas con la gestión de la vulnerabilidad técnica; incluyendo el monitoreo de la vulnerabilidad, evaluación del riesgo de la vulnerabilidad, monitoreo de activos y cualquier responsabilidad de coordinación requerida.
- El Jefe del Departamento de Tecnología e Información deberá identificar los recursos de información que se utilizarán para identificar las vulnerabilidades técnicas relevantes y mantener la conciencia sobre ellas para el software y otras tecnologías en base a una lista de inventario de activos; estos recursos de información deberán actualizarse en base a los cambios en el inventario, o cuando se encuentran recursos nuevo o útiles.
- Se deberá definir una línea de tiempo para reaccionar a las notificaciones de vulnerabilidades técnicas potencialmente relevantes.
- Una vez que se identifica la vulnerabilidad técnica potencial, el encargado de sistemas de información deberá identificar los riesgos asociados y las acciones a tomarse; dicha acción podría involucrar el parchado de los sistemas vulnerables y/o la aplicación de otros controles a realizarse por el administrador de software.
- Dependiendo de la urgencia con que se necesita tratar la vulnerabilidad técnica, la acción a tomarse deberá realizarse de acuerdo a los controles

relacionados con la gestión de cambios o siguiendo los procedimientos de respuesta ante incidentes de seguridad de la información.

5.13.- GESTIÓN DE INCIDENTES DE SEGURIDAD EN LA SEGURIDAD DE LA INFORMACIÓN

5.13.1.- Comunicación de eventos y debilidades en la seguridad de la información

Actualmente el departamento no tiene un procedimiento formal aprobado, el cual defina como los usuarios que trabajan en el Complejo y hacen uso de los activos de la Organización, sepan cómo actuar ante un evento que ponga en riesgo la seguridad de la información.

El personal conoce que debe llenar un caso en su sistema de gestión de eventos; comunicarse vía telefónica o vía correo electrónico con sus superiores; pero no existe un compromiso total, para el hecho de notificar si existe algún tipo de inconveniente o la seguridad de la información se ve comprometida.

Para lo que respecta al procedimiento que se debería implementar, en cuanto a identificar e informar, pues se debe tener en cuenta ciertas directrices entres las cuales:

- Formato de reporte de eventos en la seguridad de la información:
  - ✓ Nombre de la persona q hace la notificación del evento, incidente o falla.
  - ✓ Hora y fecha de la ocurrencia.

- ✓ Descripción del problema.
- ✓ Responsable de solucionar el problema.
- ✓ Descripción de la respuesta inicial ante el problema.
- ✓ Descripción de la solución al problema.
- ✓ Hora y fecha de solución.

- Se deberá tomar la conducta correcta en el caso de un evento en la seguridad de la información; es decir:
  - ✓ Anotar todos los detalles importantes inmediatamente.
  - ✓ No llevar a cabo ninguna acción por cuenta propia, sino reportar inmediatamente al administrador de sistemas de información.
- Retroalimentación adecuada para asegurar que aquellos usuarios que reportan eventos en la seguridad de la información sean notificados de los resultados después de haber tratado y terminado con el problema.

5.13.2.- Gestión de incidentes y mejoras en la seguridad de la información

Es necesario que el Director del Departamento de Tecnología e Información, establezca responsabilidades y el procedimiento a seguir para gestionar de manera adecuada la existencia de vulnerabilidades.

Es necesario que cada vez que se presente un evento o debilidad de la seguridad de la información, se de la alerta respectiva, se realice el análisis del porque, y se dé una solución. Para esto es necesario tomar en cuenta ciertos puntos los cuales ayudaran a que la gestión sea más eficaz:

- Se deberán establecer procedimientos para manejar los diferentes tipos de incidentes en la seguridad de la información, incluyendo:
  - ✓ Fallas del sistema de información y pérdida del servicio.
  - ✓ Código malicioso.
  - ✓ Negación del servicio.
  - ✓ Errores resultantes de datos comerciales incompletos o inexactos.
  - ✓ Violaciones de la confidencialidad e integridad.
  - ✓ Mal uso de los sistemas de información.
- Además de los planes de contingencia, los procedimientos también deberán cubrir:
  - ✓ Análisis e identificación de la causa del incidente.
  - ✓ Planeación e implementación de la acción correctiva para evitar la recurrencia, si fuese necesario.
  - ✓ Comunicaciones con aquellos afectados o involucrados con la recuperación de un incidente.
  - ✓ Reportar la acción a la autoridad apropiada.
- Se deberá recolectar y asegurar rastros de auditoría y evidencia similar, conforme sea apropiado para:
  - ✓ Análisis interno del problema.
  - ✓ Uso como evidencia forense en relación a una violación potencial del contrato o el requerimiento regulador o en el caso de una acción legal, civil o criminal.
  - ✓ Negociación para la compensación de los proveedores del software y

servicio.

- Se deberán controlar formal y cuidadosamente las acciones para la recuperación de las violaciones de la seguridad y para corregir las fallas en el sistema; los procedimientos debieran asegurar que:
  - ✓ Sólo el personal claramente identificado y autorizado tenga acceso a los sistemas vivos y los datos.
  - ✓ Se documenten en detalle todas las acciones de emergencia realizadas.
  - ✓ La acción de emergencia sea reportada a la dirección y revisada de una manera adecuada.
  - ✓ La integridad de los sistemas y controles comerciales sea confirmada con una demora mínima.

Una vez que se tenga identificado y en la mayor parte controlado la gestión de eventos y debilidades de la seguridad e la información, será necesario que el Director del Departamento de Tecnología e Información, recolecte toda la información obtenida e identifique los incidentes recurrentes o de alto impacto, y con esto verificar si es necesario implementar más controles.

Dentro de estos incidentes de la seguridad de la Información, se deben contemplar también los ejecutados por personal del Complejo o personas ajenas a la organización; ante esto es necesario crear un procedimiento el cual establezca como actuar ante este tipo de riesgos, es decir como detectarlos, el seguimiento a realizarse, toma de evidencias, etc. Cuando una acción de seguimiento contra una persona u organización después de un incidente de seguridad de la información implica acciones legales (civiles o penales), la evidencia se debe recolectar, retener y

presentar para cumplir con las reglas para la evidencia establecidas en la jurisdicción pertinente.

5.14.- GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

5.14.1.- Aspectos de la gestión de continuidad del negocio

5.14.1.1.- Proceso de la gestión de continuidad del negocio

Es necesario que como parte de los procesos que se actualmente se encuentran en desarrollo dentro del Complejo; se defina el proceso de gestión de continuidad del negocio, en el cual se definan todos requisitos de seguridad de la información necesarios.

Se detallan algunas directrices, las cuales facilitarían el desarrollo del proceso antes nombrado:

- Comprensión de los riesgos que actualmente el Complejo posee en términos de probabilidad de ocurrencia e impacto, incluyendo la identificación y priorización de los procesos críticos de los negocios.
- Comprensión del impacto que una interrupción puede tener, definición de los objetivos comerciales de las herramientas de procesamiento de información.
- Considerar la contratación de seguros que podrían formar parte del proceso de continuidad del negocio.
- Elaboración y documentación de una estrategia de continuidad consecuente con los objetivos y prioridades de los negocios acordados.
- Elaboración y documentación de planes de continuidad de conformidad con la estrategia de continuidad acordada.

- Pruebas y actualización periódicas de los planes y procesos implementados.
- Garantizar que la administración de la continuidad esté incorporada a los procesos y estructura de FAME. La responsabilidad por la coordinación del proceso de administración de la continuidad deberá ser asignada a un nivel jerárquico adecuado.

5.14.1.2.- Continuidad del negocio y análisis de impactos

Para lo que respecta a la continuidad del negocio, es necesario que se identifiquen todos los posibles eventos o incidentes que pueden suscitarse e interrumpir o parar las operaciones dentro del Complejo FAME; dentro de estos puede ser: robo de equipos e información, falla en los equipos, desastres naturales, incendios, errores intencionados o no intencionados por parte del personal, etc.

Lo siguiente a esto, es realizar una evaluación de riesgos en cual se determine la probabilidad existente de cada una de las amenazas, así como el grado de impacto que tendrían y el tiempo que tomaría retomar operaciones.

Es necesario que para esta identificación y evaluación de riesgos estén presentes cada una de las personas que conforman el directorio del Complejo, ya que solo así se podrá tomar en cuenta todos y cada uno de los recursos que están posiblemente expuestos y que deben ser resguardados de alguna manera.

Dentro de esta evaluación se deberá calificar y cuantificar los riesgos o amenazas, con esto se podrá implementar una estrategia la cual permita priorizar de acuerdo a presupuesto y tiempo la adecuación de controles.

5.14.1.3.- Redacción e implantación de planes de continuidad

Actualmente el Complejo Fame, dispone ya de un documento denominado “Plan de Contingencia informática”, al cual se le han realizado cambios hasta el mes de mayo del año 2010, se ha realizado una verificar del documento, el cual tiene ya establecido y definido los posibles riesgos, y los controles existentes para cada uno de ellos.

No será necesario redactar un nuevo documento, pero si será responsabilidad del Departamento de Tecnología e Información, que este documento siempre se encuentre actualizado

Los planes de continuidad de la ESMIL deberán ser desarrollados para mantener o restablecer las operaciones críticas de la misma en los plazos requeridos una vez ocurrida una interrupción o falla en sus procesos críticos.

5.14.1.4.- Marco de planificación para la continuidad del negocio

El plan de Continuidad del Negocio, deberá ser divido en algunos documentos, tomando en cuenta:

- Seguridad Física – Exteriores
- Seguridad Fisca – Interiores
- Seguridad en Aplicativos
- Seguridad de Información
- Seguridad en Equipos Informáticos
- Seguridad en Cableado Eléctrico y Redes

El o los objetivos generales, como la estructura de estos planes debería ser la misma, los objetivos específicos y procedimientos a llevarse a cabo deberán ser lo que difiera.

Como parte de la definición de los planes de continuidad será necesario nombrar al personal responsable que estará a cargo de cada uno de ellos. Las personas nombradas deberán estar en continua evaluación a su plan para identificar nuevos riesgos y definir controles adicionales, de igual manera llevaran a cabo pruebas o simulacros que permitan estimar el grado de eficacia del Plan de Contingencia a su cargo.

5.14.1.5.- Prueba, mantenimiento y reevaluación de planes de continuidad

Como parte del proceso de Gestión de Continuidad del Negocio, pues esta la tarea de realizar pruebas, actualizar y reevaluar el plan de continuidad.

Es importante tomar en cuenta que el personal a cargo debería tener un conocimiento amplio en cuanto a seguridad de la información se refiere, para que se logre considerar todos los requisitos del Complejo FAME.

La programación de las pruebas para los planes de continuidad del negocio debería indicar cómo y cuándo se va a probar cada elemento del plan. Para la evaluación y pruebas de cada uno de los planes es recomendable considerar algunas técnicas:

- Simulaciones, especialmente para entrenar al personal en el desempeño de sus roles de gestión posterior a incidentes o crisis.

- Pruebas de recuperación técnica, garantizando que los sistemas de información puedan ser restablecidos con eficacia.
- Pruebas de recuperación en un sitio alternativo, ejecutando procesos de negocio en paralelo, con operaciones de recuperación fuera del sitio principal.
- Pruebas de instalaciones y servicios de proveedores, garantizando que los productos y servicios de proveedores externos cumplan con el compromiso contraído.
- Ensayos completos, probando que la institución, el personal, el equipamiento, las instalaciones y los procesos pueden afrontar las interrupciones.

Los planes de continuidad deberán mantenerse mediante revisiones y actualizaciones periódicas para garantizar su eficacia permanente. Se deberían registrar los resultados de las pruebas y, cuando sea necesario, tomar las acciones para mejorar.

5.15.- CUMPLIMIENTO

5.15.1.- Conformidad con los requisitos legales

5.15.1.1.- Identificación de la legislación aplicable

Dentro de lo que respecta a requisitos legales en esta norma, y según lo identificado dentro del Complejo, pues no se tiene mayores inconvenientes, pero no está de más aclarar ciertos puntos.

Es importante que el Departamento de Tecnología e Información en conjunto con el Departamento legal, establezcan, definan y documenten todo lo relacionado a

las leyes vigentes en el país acerca de tratamiento de información, delitos informáticos, seguridad en las telecomunicaciones, marco jurídico y legislación para su uso.

5.15.1.2.- Derechos de propiedad intelectual

De igual manera es necesario recalcar en el ámbito legal los derechos de propiedad intelectual, como uno más de los procedimientos a ser desarrollados, deberá constar aquel que garantice el uso de material informático debidamente licenciado y que se tenga marcas registradas; no está por demás argumentar que el hecho de adquirir aplicaciones totalmente legales, no da el derecho de clonar, copiar, o distribuir dichos productos.

Dentro de este mismo procedimiento, se deberían recomendar capacitaciones para tratar de concientizar al personal sobre los derechos de propiedad intelectual, así como también realizar mensualmente o trimestralmente una revisión a todos los equipos informáticos para detectar la instalación de software no licenciado.

5.15.1.3.- Salvaguarda de los registros de la Organización

Toda información referente al Complejo considerada importante, como bases de datos, información legal, auditorias, transacciones, firmas electrónicas, etc. Se deberían proteger de la pérdida, destrucción y falsificación.

El almacenamiento de la información podrá ser en medios magnéticos, ópticos, etc. Pero deberán ser considerados todos los detalles en cuanto a tiempo de vida de cada uno de los medios electrónicos ocupados, así como también el tiempo

necesario que según las leyes se establece toda organización debe almacenar la información, antes de que la misma se vuelva obsoleta para la institución.

Si se seleccionan medios de almacenamiento electrónicos, el jefe del Departamento de Tecnología e Información deberá incluir procedimientos para garantizar la capacidad de acceso a los datos durante todo el período de retención, a fin de salvaguardar los mismos, así como también garantizar que esta información pueda ser extraída y leída en cualquier momento cuando las autoridades la requieran.

5.15.1.4.- Protección de datos de carácter personal y de la intimidad de las personas

Como en todo país, en Ecuador también existen en el marco legal, artículos los cuales apoyan el resguardo y protección de los datos personales

El Art. 66 de la Constitución de la República, en su parte pertinente dispone "…Se reconoce y garantizará a las personas: 19. El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos de información requerirán la autorización del titular y el mandato de la ley".

Es por esto que El Departamento De Tecnología e Información junto con el Departamento Legal deberían establecer un procedimiento el cual garantice a todo el personal que su información personal o datos íntimos estarán completamente seguros dentro de las Bases de Datos del Complejo.

5.15.1.5.- Evitar mal uso de los dispositivos de tratamiento de la información

Los servicios de procesamiento de información de una organización tienen el fin principal o exclusivo de los propósitos del negocio. Por ningún motivo, a menos que sea autorizado por la gerencia o directivos, se podrá hacer uso de estos servicios.

Es necesario que El directorio del Departamento de Tecnología e Información junto con el Departamento legal elaboren una Plantilla las cual sea firmada y entendida por todos y cada uno de los trabajadores del Complejo FAME, para formalizar el compromiso con los recursos asignados.

Además se deberán establecer métodos de monitoreo previamente estudiados por el Departamento legal quien aprobara estas técnicas y dictara las posibles sanciones a o las personas que sean detectadas realizando actividades no autorizadas.

Sera necesario también capacitar al personal para que conozcan del alcance de su acceso permitido.

5.15.1.6.- Reglamentación de los controles de cifrados

Reglamentación de cifrado o leyes en cuanto al uso de sistemas criptográficos, todavía no está muy desarrollado en el país, ni explotado como consecuencia, es por esto que antes de cualquier decisión a tomarse en cuanto al uso de este tipo de controles o sistemas, se debería buscar asesoría legal para garantizar el cumplimiento con las leyes y los reglamentos nacionales.

5.15.2.- Revisiones de la política de seguridad y de la conformidad técnica

En cuanto a la política de seguridad, es necesario que por parte de los directivos de cada uno de los departamentos se realice una revisión periódica no mayor a tres meses, en las cuales se determine si los procedimientos de seguridad definidos se estén cumpliendo de manera correcta y sin excepciones.

Si fuese el caso de existir inconvenientes o incumplimientos, pues se debería realizar un análisis de por qué no se ha ejecutado lo pedido, implementar técnicas de corrección y hacer conocer al personal del error cometido.

En cuanto a conformidad técnica se refiere, pues se deberán efectuar revisiones trimestrales en las cuales se evalúe si todos los controles de hardware y software han sido o están siendo implementados de manera correcta. Es recomendable que este proceso lo realice personal experto en el tema para que así no se ponga en peligro los sistemas que en producción se encuentran.

5.15.3.- Consideraciones sobre la auditoria de sistemas

Los directivos de cada departamento, junto con la gerencia del Complejo deberán reunirse y planificar con un tiempo prudencial, la ejecución de auditorías, tanto por personal interno como por personal externo, ambos especializados para minimizar interrupciones a la operación diaria del Complejo.

Toda actividad realizada dentro de una auditoria, deberá ser monitoreada y registrada, para generar una bitácora de rastro, la cual permita identificar qué y cuándo se evaluó cual departamento o procedimiento.

Cuando se realicen las auditorias y se haga uso de aplicaciones, es recomendable se aísle estos sistemas de la infraestructura en producción para que las mismas no adquieran un riesgo de ser usadas por personal no autorizado.

CAPÍTULO VI

CONCLUSIONES Y RECOMENDACIONES

6.1 CONCLUSIONES

- La metodología PETI mediante el análisis administrativo, ha permitido identificar y comprender la Estrategia de Negocio de la Empresa Fame S.A., puntal fundamental para el desarrollo la Estrategia de Tecnologías de Información.

- La empresa Fame S.A., no cuenta con un departamento de Tecnología e Información propio. El departamento actual brinda soporte a todas las empresas del Complejo Industrial, esto lleva, a que el análisis de los requerimientos de Tecnologías de Información se lo realice de manera estandarizada, y al tener cada empresa un giro de negocio diferente, dicho análisis puede no tomar en consideración requerimientos puntuales originados por el giro de negocio mismo.

- El Departamento de Tecnología e Información, no cuenta con procedimientos escritos, se deja libre al conocimiento y paso de información entre integrantes del equipo; lo cual pone fácilmente en riesgo la seguridad de la información.

- El tema de Seguridad de la Información dentro del Complejo tiene muchas falencias, ya que no se ha dado la importancia que amerita. Para muchas

empresas al igual que lo que se ha visto en la evaluación realizada a FAME, la Seguridad de la Información está ligada a realizar respaldos de la información y mantenerlos seguros; sin darse cuenta que en realidad existen muchos puntos adicionales los cuales necesitan ser revisados ya que generan infinidad de riesgos y pueden llegar a ocasionar problemas graves para la organización sino se implementan los respectivos controles.

6.2 RECOMENDACIONES

- Aplicar y difundir la metodología PETI para el desarrollo y seguimiento de los proyectos de Sistemas de Información planteados en el Plan Estratégico de Tecnologías de Información y proyectos futuros.

- Formar o reestructurar el departamento de Tecnología e Información, de manera que, se enfoque a la estructura organizacional de FAME, y este en la capacidad de entender su giro de negocio y atender sus requerimientos puntuales.

- La Gerencia General junto a cada uno de los directores de Departamento del Complejo, de manera urgente deberían realizar reuniones en las cuales puedan determinar que procesos y que procedimientos dentro de la Organización, no han sido documentados formalmente. Para nuestro estudio se ha detectado algunos procedimientos que solo existen por conocimiento general, los mismos permiten que se vayan presentando mas y mas riesgos, por ende amenazas a la Seguridad de la Información.

- Implementar las recomendaciones y buenas prácticas definidas en este documento guiados por la ISO 27002 para poder mantener una gestión de Seguridad de Información adecuada, correctamente monitoreada, evaluada y corregida en caso de ser necesario dando así cumplimiento a la norma de control gubernamental de tecnologías de la información.

BIBLIOGRAFÍA

- ANDREU, Rafael & Ricand, Joan. Estrategia y Sistemas de Información. Segunda Edición. McGraw Hill.
- Plan Estratégico Informático del Ejército del Ecuador.
- MINTZBERG,H., Quinn, J. El proceso Estratégico, De. Prentice may, segunda edición, 1993.
- www.degerencia.com/articulo/diagnostico_estrategico_dofa
- www.slideshare.net/concepto-de-arquitectura-de-tecnologias-de-informacion
- www.monografias.com/
- www.mideplan.go.cr/sinades/Proyecto_SINADES/capacitacion
- ControlesISO17799-2005
- EAR - Herramientas para el Análisis de Riesgos
- Manual de Políticas de Seguridad Informática Inf-Tek Gerencia de Tecnologías de Información
- Análisis de riesgos ISO 27005 vs magerit y otras metodologías GestioPolis
- MAGERIT – versión 2_ Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información
- Código de práctica para la administración de la seguridad de la información: Instituto argentino de normalización
- Código de práctica para la administración de la seguridad de la información: Instituto colombiano de normalización
- Código de práctica para la administración de la seguridad de la información: Instituto español de normalización

BIOGRAFÍA

DATOS PERSONALES

Nombres y Apellidos:	José Luis Rojas Urgilés
Lugar y Fecha de Nacimiento:	Quito, 27 de mayo de 1984
Cedula de Identidad:	171782631-5
Estado Civil:	Soltero
Dirección:	Sangay 248 y García Moreno, Valle de los Chillos
Teléfono:	092668711
E-mail:	zeluiz_01@hotmail.com

FORMACIÓN ACADÉMICA

Primaria

Farina Quito-Ecuador

Secundaria

Colegio San Gabriel Quito-Ecuador

Superior

ESPE Ingeniería en Sistemas

CURSOS

2004 – Participación en el I Congreso Nacional de Sistemas e Informática ESPE

2005 – Participación Minicurso de Arquitectura .NET en el I Congreso Nacional de Sistemas e Informática ESPE 2005.

2007 – Congreso Informático ESPE → Ingeniería de requisitos, Data Ware House.

DATOS PERSONALES

Nombres y Apellidos:	Juan José Vela Veintimilla
Lugar y Fecha de Nacimiento:	Loja, 9 de Diciembre de 1985
Cedula de Identidad:	110276580-5
Estado Civil:	Soltero
Teléfono:	098353382 022864694
Dirección Domiciliaria:	San Rafael, Psj. Calderón 501 y Calle Río Napo.
E-mail:	juanjo_vela2@hotmail.com

FORMACIÓN ACADÉMICA

Estudios Primarios

Escuela Miguel Ángel Suárez (Loja, 1997)

Estudios Secundarios

Colegio Militar “Lauro Guerrero”, Loja

Pedro Ruiz Gallo (Lima - Perú)

Colegio Militar “Eloy Alfaro”, Quito

Estudios Universitarios

Escuela Superior Politécnica del Ejército

CURSOS

2004 – Participación en el I Congreso Nacional de Sistemas e Informática ESPE

2005 – Participación Minicurso de Arquitectura .NET en el I Congreso Nacional de Sistemas e Informática ESPE 2005.

2007 – Congreso Informático ESPE → Ingeniería de requisitos, Data Ware House.

HOJA DE LEGALIZACIÓN DE FIRMAS

ELABORADA(O) POR

_____

Sr. José Luis Rojas Urgilés

_____

Sr. Juan José Vela Veintimilla

DIRECTOR DE LA CARRERA

_____

Ing. Mauricio Campaña

SANGOLQUÍ, 9 de Noviembre de 2011.