UNIVERSIDAD POLITÉCNICA SALESIANA

FACULTAD DE INGENIERÍAS
SEDE QUITO- CAMPUS SUR

CARRERA DE INGENIERÍA EN SISTEMAS
MENCIÓN TELEMÁTICA

TÍTULO DE LA TESIS DE GRADO

"Investigación y propuesta de un modelo de gestión mediante el análisis de las Normas ISO 27000 e ISO 9000, que garantice la seguridad y calidad en los procesos de diseño, construcción y ejecución de software en una mediana empresa de desarrollo de sistemas informáticos (**LST Logística y Servicios Tecnológicos**),**".**

TESIS PREVIA A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS

ELABORADO POR:
CRISTHIAN VINICIO URIBE CISNEROS

DIRECTOR DE TESIS:
Ing. Franklin Hurtado

QUITO – PICHINCHA – ECUADOR

Diciembre 2010

DECLARACIÓN

Yo URIBE CISNEROS CRISTIAN VINICIO, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la Universidad Politécnica Salesiana, según lo establecido por la ley de propiedad intelectual, por su reglamento y por la normatividad institucional vigente.

_____

Uribe Cisneros Cristian Vinicio

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Uribe Cisneros Cristian Vinicio, bajo mi dirección.

_____

Ing. Franklin Hurtado
Director de Tesis

AGRADECIMIENTO.

A Dios, por estar conmigo en cada paso que doy, por fortalecer mi corazón e iluminar mi mente.

A mis padres Marcial y Rosa por su amor, su entrega incondicional, por su apoyo en todo sentido para la consecución de mis más grandes sueños.

A mis hermanos Mishell y Bryan por ser fuente de ternura, cariño y apoyo en todo momento.

A mi esposa Andrea por compartir el día a día con amor, paciencia y cariño apoyándome y motivándome a seguir adelante.

A la Universidad Politécnica Salesiana por guiarme en todo mi desarrollo profesional además prestarme su apoyo y confianza para el desarrollo de este trabajo.

Al Ingeniero Franklin Hurtado por su acertada dirección, conocimientos prestados, sugerencias y por ser un gran motivador durante la elaboración de éste trabajo.

.

A todas aquellas personas que de una u otra forma colaboraron para hacer de este sueño una realidad.

DEDICATORIA.

Dedico la presente tesis a mi hijo Ariel Alexander que bajo del cielo, para llenar de alegría mi vida, gracias porque eres mi inspiración y fortaleza, una sonrisa tuya ilumina mi mundo y me da las fuerzas necesarias para luchar y conseguir mis metas.

ÍNDICE GENERAL

CAPÍTULO V

ÍNDICE DE ABREVIATURAS

BSI	British Standards Institution
BUGS	Error de software
CAD	Diseño Asistido por Computadora
COPYLEFT	Forma de licencia, usado para modificar el derecho de autor
CPU	Unidad Central de Procesamiento
CSI	Instituto de Seguridad Informática
DBMS	Sistemas de Gestión de Bases de Datos
DFD	Diagrama de Flujos de Datos
DIN	Instituto Alemán de Normalización
FTP	Protocolo de Transferencia de Archivos
GUI	Interfaz Gráfica de Usuario
IEC	Comisión Electrotécnica Internacional
IEEE	Instituto de Ingenieros Electricistas y Electrónicos
IPS	Sistema de Prevención de Intrusos
ISO	La Organización Internacional para la Estandarización
LST	Logística y Servicios Tecnológicos
MC	Manual de Calidad
MP	Mapa de Procesos
MS-DOS	Sistema operativo de disco de Microsoft
NIST	Instituto Nacional de Estándares y Tecnología
PDCA	Planificar, Hacer, Verificar, Actuar
PMP	Project Managment for Professionals
POST	Power On Self Test (auto prueba de encendido)
PSI	Política de seguridad Informática
RC	Release Candidate
RRHH	Recursos Humanos
RTM	Release to Manufac (Aptitud para el Fabricante)
SGC	Sistema de Gestión de Calidad
SGSI	Sistema de Gestión de Seguridad de la Información.
SO	Sistemas Operativos
WEBSOFT	Software a medida

ÍNDICE DE FIGURAS

ABSTRACT

Dada la evolución de la tecnología y su relación directa con los objetivos del negocio de una organización, el universo de amenazas y vulnerabilidades aumenta, por tanto se vuelve una necesidad el proteger dos de los activos más importantes de una empresa, la calidad y la información, garantizando siempre la disponibilidad, la confidencialidad e integridad de las mismas. La forma adecuada para satisfacer a los clientes y proteger la seguridad de la información es mediante un correcto Sistema de Gestión de Calidad y un Sistema de Seguridad de la Información, respectivamente, logrando así identificar y focalizar esfuerzos hacia aquellos elementos que se encuentren más expuestos.

Para esto se ha trabajado con LST Logística y Servicios Tecnológicos, una organización dedicada a diversas áreas de tecnología y gestión de proyectos, haciendo una verificación de su situación actual, y observando cuales son los puntos donde se encuentran la mayoría de sus falencias, para mediante estos análisis, elaborar: primero un manual de Gestión de Calidad, con el fin de eliminar problemas y corregir ciertos aspectos que se los desempeña mal dentro de la empresa, y segundo un Manual de Gestión de Seguridad de la Información, con el propósito de reducir los serios problemas que LST tiene con respecto a la información.

Todo el trabajo presentado a continuación, cuando sea implementado permitirá a LST desempeñar sus actividades diarias de manera ordenada, con calidad y seguridad, con el fin de obtener la satisfacción de sus clientes.

Para esta propuesta se ha establecido como base los requisitos de la norma ISO 9001:2008 e ISO 27001:2005.

CAPÍTULO I

DATOS INFORMATIVOS DEL PROYECTO

1. TITULO DE LA INVESTIGACIÓN.

Investigación y propuesta de un modelo de gestión mediante el análisis de las Normas ISO 27000 e ISO 9000, que garanticen la seguridad y calidad en los procesos de diseño, construcción y ejecución de software en una mediana empresa de desarrollo de sistemas informáticos (**LST Logística y Servicios Tecnológicos**)**.**

2. PLANTEAMIENTO DEL PROBLEMA

Si bien las metodologías y estándares relacionados con el desarrollo y construcción de software buscan mantener altos niveles de confiabilidad y control de la solución informática, la seguridad de la información así como los estándares de calidad no son necesariamente parte formal de dichos estándares.

En este sentido, la formalidad en la evaluación del diseño de la solución desde el punto de vista de seguridad podría verse comprometida, dado que no se encuentran claros criterios de análisis en este sentido, debido a causas como una escasa apertura administrativa por parte de la empresa en cuanto a estándares de seguridad de la información; Una limitada predisposición por parte de la empresa, ante la necesidad de superar un proceso de calificación y certificación que se ejecuta a largo plazo y un mínimo conocimiento respecto a la importancia de los estándares, que permiten mantener altos niveles de confiabilidad y control de la información. (**Ver anexo 1**).

Estas razones traen como consecuencias o efectos el que se presente como un inconveniente para los creadores del software, porque le resta

competitividad; Se permita la posibilidad de abrir brechas de seguridad en los sistemas o se comprometa la formalidad en la evaluación del diseño de la solución desde el punto de vista seguridad, dado que no se encuentran claros criterios de análisis en este sentido.

2.1. Formulación del problema

¿Cómo la investigación respecto a normas sobre seguridad de la información, y la gestión de calidad ayudará a resolver en forma eficaz, efectiva y técnicamente accesible, la adopción e implementación de modelos de gestión de calidad y de estándares autorizados internacionales, previo el diseño, construcción e implementación de software para la empresa LST Logística y Servicios Tecnológicos, en el Ecuador?

Buena parte de las empresas de desarrollo de software del país no cuentan con un modelo de calidad y gestión de seguridad además de estándares de productos.

2.2. Sistematización del problema

¿Cuándo es el momento adecuado para determinar, que los resultados de esta investigación van a permitir tener una solución, respecto a las inquietudes de empresarios y diseñadores y la adopción de los estándares de seguridad informática?

¿Dónde sería más útil la información que se obtenga producto de este trabajo investigativo?

¿Cómo se pueden utilizar los conocimientos, recursos y técnicas informáticas necesarias, para trabajar con una matriz que dispongan los estándares de seguridad informática y gestión de calidad?

¿Por qué se cree, que existe la necesidad de investigar sobre el tema de estándares de seguridad y gestión de calidad en el diseño, construcción y

ejecución de software en una empresa?

3. OBJETIVOS;

3.1. Objetivo General

Proponer un modelo de gestión de seguridad y calidad en base a la investigación de las normas internacionales ISO 27000 e ISO 9000, dirigido a la empresa (**LST Logística y Servicios Tecnológicos**) para que tenga un mejor control en sus procesos de ingeniería.

3.2. Objetivos Específicos

- Investigar y analizar todos los puntos que constituyen y forman parte de las normas ISO 27001 e ISO 9001.
- Estudiar la situación actual de la empresa **LST Logística y Servicios Tecnológicos** en cuanto a la seguridad y gestión de calidad en el diseño, construcción y ejecución de software.
- Investigar sobre los beneficios que trae trabajar con un modelo de gestión establecido dando énfasis a la seguridad y calidad en software.
- Proponer un modelo de gestión de seguridad y calidad informática, mediante un resumen, basado en la información de los estándares ISO 27001 e ISO 9001.
- Lleva a cabo el proyecto en base a la metodología PMP.

4. JUSTIFICACIÓN

Justificación Práctica

La seguridad informática siempre será motivo de estudio, ya que tiene como fin la protección de la información y de los sistemas de la información del acceso, uso, divulgación, interrupción o destrucción no autorizada de la misma, debido a su particularidad de ser vulnerable permanentemente. Considerando que

había la necesidad de realizar una investigación en torno a los estándares que garantizan la solvencia de un software, se escogió el tema del diseño, construcción y ejecución de software sometidos a la normativa referente especialmente las normas ISO 27001 e ISO 9000, por lo que se cree que la información que se genere en la presente investigación, puede ser utilizada, para tomar medidas tendientes a mejorar el sector antes mencionado.

Si bien es cierto el presente trabajo, no pretende presentar una solución definitiva al problema planteado, al menos se va a realizar una recopilación de la información referente al tema, y la propuesta de un modelo de gestión que de aplicarse contribuirá como una guía para emplear la seguridad y calidad del software tanto en el proceso de desarrollo, como en el producto final que produzca la empresa **LST Logística y Servicios Tecnológicos**, por lo que esta investigación en ese sentido si se reviste de una justificación práctica.

Justificación Teórica

Al estudiar el tema de la seguridad informática, es necesario buscar aportes teóricos que soporten todos los análisis que se presenten. Sin embargo el propósito de este trabajo es generar reflexión y debate relacionado con el tema, con la participación directa de diseñadores y ejecutores del software, dentro de un marco normativo basado en los estándares:

- ✓ ISO 27001: Tecnologías de Información, Técnicas de Seguridad, Sistemas de gestión de la seguridad de la información y requerimientos.

- ✓ ISO 9000: Sistemas de Gestión de la Calidad - Conceptos y Vocabulario.

En todo caso, como afirma López Cerezo, toda investigación en alguna medida tiene la doble implicación, teórica y práctica[1]; y existiendo la intención de generar reflexión y debate, sobre el conocimiento disponible, confrontando

[1] LÓPEZ CEREZO, José A., "Filosofía crítica de la ciencia", Antropos, No 82-83, Barcelona, 1988.

información de varios autores, entonces se puede afirmar que existe una justificación teórica.

Justificación Metodológica

Y finalmente se puede mencionar que existe una justificación metodológica debido a que, la recopilación de información y análisis por realizar, respecto a los estándares ISO 27001 e ISO 9000 se circunscribe a analizar los procedimientos metodológicos que se tiene que seguir al momento de diseñar, construir y ejecutar un software, hasta alcanzar una calificación internacional.

5. ALCANCE DEL PROYECTO

El alcance del proyecto es el de recopilar y analizar toda la información referente a la seguridad informática y la gestión de calidad, en este sentido se establece como marco de trabajo la descripción de lo que se maneje en la empresa **LST Logística y Servicios Tecnológicos**

Esta investigación abarca el estudio de las normas o estándares internacionales como hitos para la gestión de calidad y de la seguridad de la información. En el caso particular del diseño, construcción y ejecución de software se seleccionan la Norma Técnica INTE-ISO 27001 e ISO 9001.

El trabajo de investigación consiste en presentar un marco teórico y un modelo, con la finalidad de que la Empresa **LST (Logística y Servicios Tecnológicos**) tome este trabajo como referencia básica y realice aplicaciones prácticas en base a las normas de seguridad y gestión de calidad mencionadas.

De igual forma con la finalidad de delimitar claramente el trabajo, y hasta donde se quiere llegar, este va a tener como referencia lo enunciado en la pregunta de investigación: ¿Cómo la investigación respecto a normas sobre seguridad informática y gestión de calidad, ayudarán a resolver en forma eficaz, efectiva y técnicamente accesible, la adopción e implementación de seguridad y calidad informática tanto en el proceso de desarrollo del software,

como en el producto final, para **LST (Logística y Servicios Tecnológicos**) en el Ecuador?

De tal manera que la información que se genere en la presente investigación, va a aportar con conocimientos actualizados, que servirán como base para que otros investigadores y demás personas involucradas tomen como referencia para elegir decisiones o ampliar investigaciones posteriores.
No emitiremos especificaciones de producto, salvo en los temas de seguridad pues nos enfocaremos principalmente a los procesos de desarrollo.

6. METODOLOGÍA

6.1. Investigación

6.1.1 Unidad de análisis

Las unidades de análisis del presente estudio, consideradas como un conjunto de elementos serán: el proceso de adoptar e implementación la aplicación de un estándar internacional respecto a la seguridad informática, y a la gestión de calidad con el soporte teórico disponible, y los Organismos relacionados con el tema.

Tratándose de un tema específico como es, Investigación de los estándares que garanticen la seguridad y calidad de la información en el diseño, construcción y ejecución del software para una mediana empresa, y considerándose de que al final de la investigación se debe recomendar un resumen suficiente acerca de la información recopilada, entonces dicha información básica es otro de los elementos que forma parte del proceso.

6.1.2 Métodos de investigación

Entre los métodos que se han seleccionado para la recolección de información en la presente tarea, están:

- **Análisis.**

Se puede decir que consiste en la identificación de cada una de las partes de la realidad y su relación, separando el objeto de estudio en dos partes y, una vez comprendida su esencia, construir un todo[2].

Se trata de la Identificación de cada una de las partes que componen el proceso técnico que se sigue para diseñar, construir y ejecutar un software, bajo estándares internacionales de seguridad informática, es decir, las diferentes etapas y técnicas a aplicarse.

- **Deductivo**

Es un proceso analítico sintético que presentan conceptos, definiciones, leyes o normas generales, de las cuales se extraen conclusiones o se examina casos particulares sobre la base de afirmaciones generales ya presentadas.

En este caso, se puede decir que se pretende investigar el principio de las normas o estándares con reconocimiento internacional, y dentro de ellas las correspondientes a seguridad informática ISO 27001.

6.1.3. Tipo de investigación

El presente estudio de investigación está clasificado como un diseño no experimental porque el investigador se limita a levantar información teórica, y permitir que éstas sean receptadas y ampliadas por parte de otras personas interesadas sin intervenir en su desarrollo.

- **Enfoque**

El presente trabajo se realiza dentro de una concepción Cualitativa ya que se trata de recopilar información y rescatar conceptos a considerarse dentro de un Programa posterior.

[2] Franco S., Cursos on-line (2009) emagister.com. Tomado de http://www.emagister.com/cursos-gratis/emag_users/solicitudes/index.cfm

- **Nivel de investigación**

Tratándose de la implementación de un tema actual como la adopción de estándares de seguridad informática, el nivel de esta Investigación es Exploratorio porque pretende explorar el conocimiento sobre una realidad o fenómeno que no ha sido suficientemente estudiado, o que no existe suficiente evidencia empírica y teórica[3].

6.1.4. Técnicas e instrumentos de investigación

Entre las técnicas e instrumentos de recolección de datos, se destacan: la entrevista y las Observaciones de Campo.

- **Entrevistas a profundidad**

La Entrevista es un procedimiento utilizado especialmente en la investigación de corte teórico; es una conversación dirigida entre dos o más personas en donde la persona entrevistada es la fuente principal de la información[4].

Este instrumento de investigación consiste en la elaboración de preguntas dirigidas a expertos escogidos en forma no aleatoria y se ha recurrido a un formulario o cuestionario que orienta la conversación, las mismas que están diseñadas en función de los objetivos de la investigación.

- **Observaciones de campo**

Se basa en la realización de observaciones personales por parte del investigador, en sitios afines al tema, es decir, donde se realizan actividades de desarrollo de software, con la finalidad de recoger información y determinar los posibles datos observadas de primera mano.

[3] Vejarano G, (2009) Asignatura Metodología de la investigación, Maestría en Educación y Desarrollo Social. UTE. Quito
[4] Ibidem

6.1.5. Aplicación de los instrumentos de investigación

Una vez que se ha seleccionado la entrevista y la observación de campo como instrumentos de medición confiables y validos, se procederá a condensar la información del tema de estudio, conociendo de esta manera, sus opiniones, actitudes y sugerencias respecto al tema, además de observaciones de interés que conllevan a esclarecer el planteamiento de soluciones desde una óptica diferente.

Con la recopilación y planteamiento de la información teórica de la investigación, más los análisis obtenidos a través de las entrevistas a expertos y la observación de campo por parte del investigador, se completa la información necesaria que sustentará el presente trabajo investigativo, permitiendo de esta manera plantear recomendaciones y sugerencias correspondientes, en la última parte del trabajo.

Fuentes de información

En el presente trabajo se distinguen dos tipos fundamentales de fuentes de información: Fuentes primarias y fuentes secundarias.

En el presente caso investigativo, como *fuentes primarias* utilizadas se destacan: Recopilación teórica realizada por la investigadora en libros relacionados con el tema de seguridad informática, artículos de revistas especializadas, memorias de seminarios y talleres especializados.

Como *fuentes secundarias* se han tomado los datos recopilados y procesados por otros investigadores que a su vez la han adaptado en investigaciones similares o afines a la presente, tales como artículos publicados en Internet, Guías, diccionarios especializados y base de datos bibliográficos.

6.2. Gestión del proyecto

6.2.1. PMP

Es un modelo de fases que nos puede ayudar a:

- Pronosticar costos y gastos para un resultado final más preciso
- Rastrear programas, recursos, presupuestos para cumplir con los objetivos del proyecto
- Identificar problemas potenciales para mantener bajos costos
- Asignar y gerenciar efectivamente al personal para maximizar recursos
- Estandarizar las mejores prácticas para una mayor eficiencia

Para este proyecto utilizare PMP mediante un modelo de fases de tipo CASCADA.

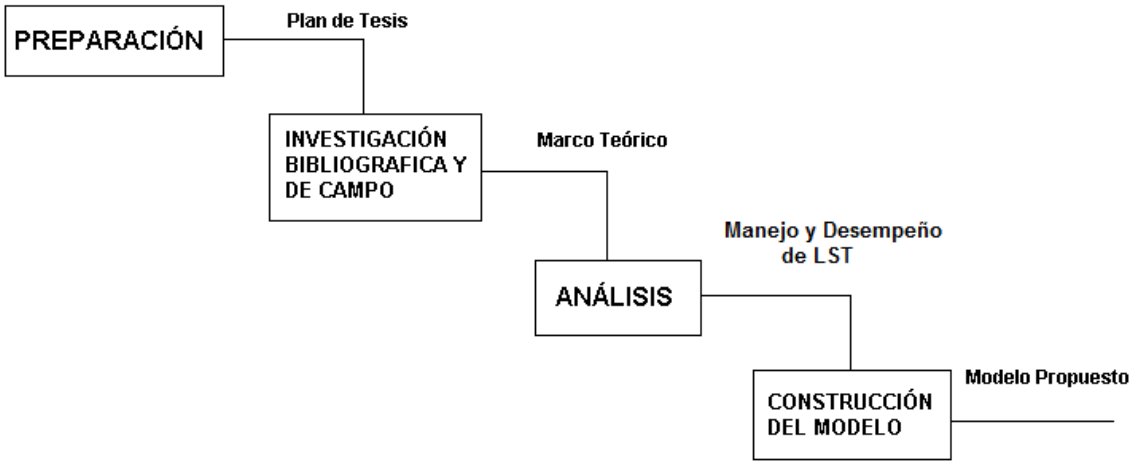


Figura #1. Modelo de fases PMP de tipo Cascada

7. TEMAS AFINES DESARROLLADOS

a) Tesis

Tema: Plan estratégico de seguridad de la información para el Departamento de Tecnología de Información del Poder Judicial, basado en el estándar ISO 27001.

Autor: Helberth Marín Hernández

Institución: Instituto Tecnológico de Costa Rica, Departamento de Computación, Programa de Maestría.

b) Tesis:

Tema: Seguridad para lograr Confiabilidad y Calidad de los Servicios digitales en Internet.

Universidad de las Américas Puebla

Autor: Carlos Augusto Jerez Lugo

CAPÍTULO II

2. MARCO TEÓRICO

2.1. DESARROLLO DE SOFTWARE

A manera de introducción podemos decir que al hablar del software en una empresa u organización, estamos refiriéndonos al conjunto de aplicaciones informáticas que permiten operar, controlar, gestionar y administrar la información.

2.1.1. DEFINICIÓN DE SOFTWARE.

El software simboliza un grupo de instrucciones que las computadoras emplean para manipular datos. Sin el software, la computadora sería un conjunto de medios inútiles.

Cuando introducimos software a una computadora, nos podemos dar cuenta que como por arte de magia hemos alimentado de conocimientos a ésta ya que en seguida comienza a operar como si pudiera pensar. Esto debido a que realiza muchas tareas sí sola, tareas como: cálculos, registros, procesamiento de datos, etc.

El Software es un conjunto de programas, documentos, procedimientos, y rutinas asociados con la operación de un sistema de cómputo. Distinguiéndose de los componentes físicos llamados hardware.

2.1.1.1. TIPOS O CLASIFICACIONES DEL SOFTWARE

El software se clasifica en 4 diferentes Categorías:

a) SISTEMAS OPERATIVOS

El sistema operativo es el que se encarga de administrar y organizar todas las

actividades que realiza la computadora. Marca las pautas según las cuales se intercambia información entre la memoria central y la externa, y determina las operaciones elementales que puede realizar el procesador. El sistema operativo, debe ser cargado en la memoria central antes que ninguna otra información.

b) LENGUAJES DE PROGRAMACIÓN

Con los programas ordenamos a la computadora que tarea debe realizar y cómo efectuarla, pero para ello es preciso introducir estas órdenes en un lenguaje que el sistema pueda entender. En principio, el ordenador sólo entiende las instrucciones en código máquina, es decir, el específico de la computadora. Sin embargo, a partir de éstos se elaboran los llamados lenguajes de alto y bajo nivel.

c) SOFTWARE DE USO GENERAL

El software de uso general brinda la estructura para un gran número de aplicaciones empresariales, científicas y personales. El software de hoja de cálculo, de diseño asistido por computadoras (CAD), de procesamiento de texto, de manejo de Bases de Datos, pertenece a esta categoría. La mayoría de software para uso general se vende como paquete; es decir, con software y documentación orientada al usuario (manual de referencia, plantillas de teclado y demás).

d) SOFTWARE DE APLICACIONES

El software de aplicación está diseñado y escrito para realizar tareas específicas personales, empresariales o científicas como el procesamiento de nóminas, la administración de los recursos humanos o el control de inventarios. Todas éstas aplicación es procesan datos (recepción de materiales) y generan información (registros de nómina) para el usuario.
(**Algunos autores consideran la 3era y 4ta clasificación como una sola**).

2.1.2. CARACTERÍSTICAS DEL SOFTWARE DESARROLLADO

Los sistemas informáticos implementados deben seguir un estricto proceso de ingeniería, basado en estándares, y documentando cada una de las fases del desarrollo.

Entre las características importantes mencionamos las siguientes:

- Diseño, implementación e implantación de acuerdo sus necesidades
- Flexibilidad y Escalabilidad
- Tecnología de punta acorde a su infraestructura
- Garantía extendida
- Soporte técnico inmediato
- Capacitación especializada

2.1.3. FASES DEL PROCESO DE DESARROLLO DEL SOFTWARE

Figura#2. Fases del proceso de desarrollo del software.
Fuente: http://jhomo.blogspot.es/1272753909/

Análisis de requisitos

Extraer los requisitos de un producto de software es la primera etapa para crearlo. Mientras que los clientes piensan que ellos saben lo que el software tiene que hacer, se requiere de habilidad y experiencia en la ingeniería de

software para reconocer requisitos incompletos, ambiguos o contradictorios. El resultado del análisis de requisitos con el cliente se plasma en el documento ERS, Especificación de Requerimientos del Sistema. Asimismo, se define un diagrama de Entidad/Relación, en el que se plasman las principales entidades que participarán en el desarrollo del software. La captura, análisis y especificación de requisitos (incluso pruebas de ellos), es una parte crucial; de esta etapa depende en gran medida el logro de los objetivos finales. Se han ideado modelos y diversos procesos de trabajo para estos fines. Aunque aún no está formalizada, ya se habla de la Ingeniería de Requisitos.

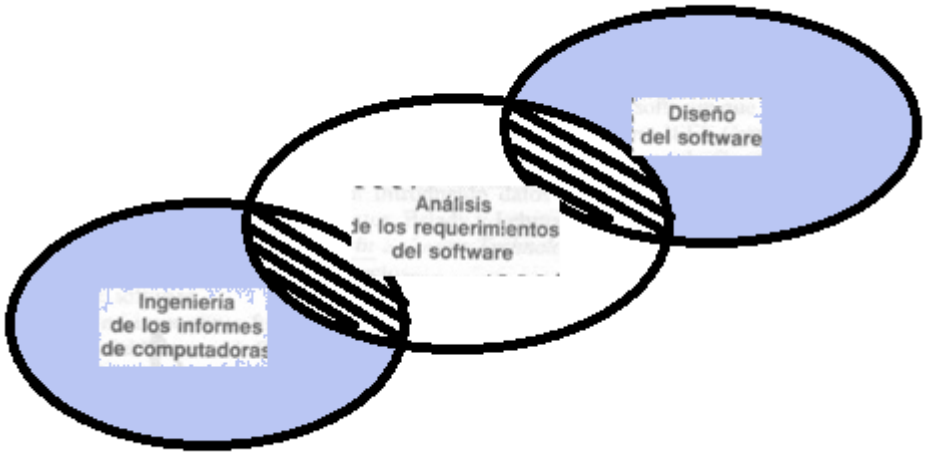


Figura #3. Tareas planteadas por la asignación de software.

Diseño y arquitectura

Se refiere a determinar cómo funcionará de forma general sin entrar en detalles. Consiste en incorporar consideraciones de la implementación tecnológica, como el hardware, la red, etc. Se definen los Casos de Uso para cubrir las funciones que realizará el sistema, y se transforman las entidades definidas en el análisis de requisitos en clases de diseño, obteniendo un modelo cercano a la programación orientada a objetos.

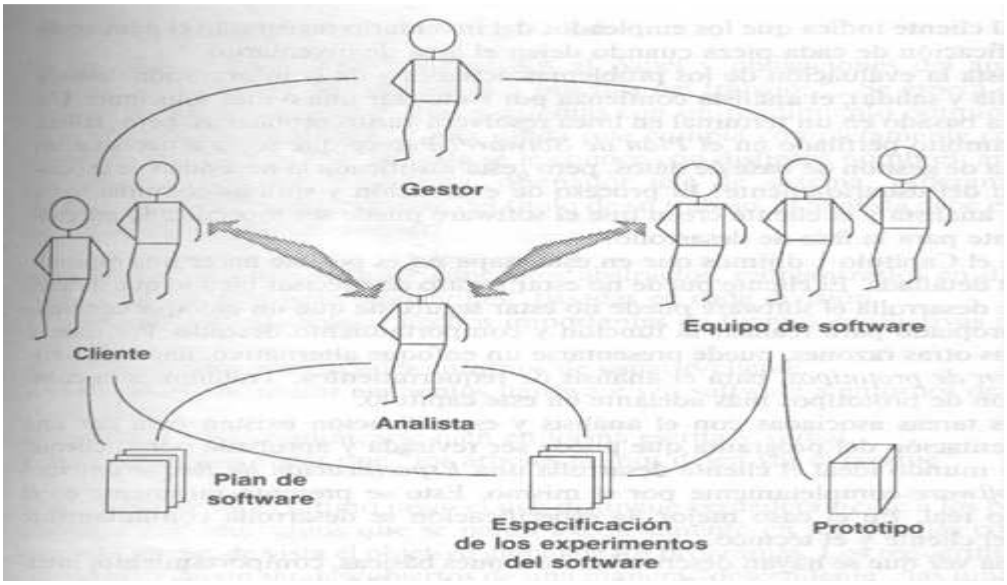


Figura #4. Comunicación en el proceso de desarrollo de software
Fuente: http://www.monografias.com/trabajos5/desof/desof.shtml

Programación

Reducir un diseño a código puede ser la parte más obvia del trabajo de ingeniería de software, pero no es necesariamente la porción más larga. La complejidad y la duración de esta etapa está íntimamente ligada al o a los lenguajes de programación utilizados.

Pruebas

Consiste en comprobar que el software realice correctamente las tareas indicadas en la especificación. Una técnica de prueba es probar por separado cada módulo del software, y luego probarlo de forma integral, para así llegar al objetivo.

Se considera una buena práctica el que las pruebas sean efectuadas por alguien distinto al desarrollador que la programó, idealmente un área de pruebas; sin perjuicio de lo anterior el programador debe hacer sus propias pruebas. En general hay dos grandes formas de organizar un área de pruebas, la primera es que esté compuesta por personal inexperto y que desconozca el tema de pruebas, de esta forma se evalúa que la documentación entregada sea de calidad, que los procesos descritos son tan claros que cualquiera puede

entenderlos y el software hace las cosas tal y como están descritas. El segundo enfoque es tener un área de pruebas conformada por programadores con experiencia, personas que saben sin mayores indicaciones en qué condiciones puede fallar una aplicación y que pueden poner atención en detalles que personal inexperto no consideraría.

Documentación

Todo lo concerniente a la documentación del propio desarrollo del software y de la gestión del proyecto, pasando por modelaciones (UML), diagramas, pruebas, manuales de usuario, manuales técnicos, etc.; todo con el propósito de eventuales correcciones, usabilidad, mantenimiento futuro y ampliaciones al sistema.

Mantenimiento

Mantener y mejorar el software para enfrentar errores descubiertos y nuevos requisitos. Esto puede llevar más tiempo incluso que el desarrollo inicial del software. Alrededor de 2/3 de toda la ingeniería de software tiene que ver con dar mantenimiento. Una pequeña parte de este trabajo consiste en arreglar errores, o bugs. La mayor parte consiste en extender el sistema para hacer nuevas cosas.

2.1.4. ETAPAS DEL PRODUCTO DESARROLLADO

En la ingeniería del software el término **etapas** expresa cómo ha progresado el desarrollo de un software y cuánto desarrollo puede requerir. Cada versión importante de un producto pasa generalmente a través de una etapa en la que se agregan las nuevas características (etapa alfa), después una etapa donde se eliminan errores activamente (etapa beta), y finalmente una etapa en donde se han quitado todos los bugs importantes (etapa estable). Las etapas intermedias pueden también ser reconocidas. Las etapas se pueden anunciar y regular formalmente por los desarrolladores del producto, pero los términos se utilizan a veces de manera informal para describir el estado de un producto.

Normalmente muchas compañías usan nombres en clave para las versiones antes del lanzamiento de un producto, aunque el producto y las características reales son raramente secretas.

ALFA

Es la primera versión del programa, la cual es enviada a los verificadores para probarla.

Algunos equipos de desarrollo utilizan el término **alfa** informalmente para referirse a una fase donde un producto todavía es inestable, aguarda todavía a que se eliminen los errores o a la puesta en práctica completa de toda su funcionalidad, pero satisface la mayoría de los requisitos.

El nombre se deriva de alfa, la primera letra en el alfabeto griego.

BETA

Una **versión beta** o **lanzamiento beta** representa generalmente la primera versión completa del programa informático o de otro producto, que es posible que sea inestable pero útil para que las demostraciones internas y las inspecciones previas seleccionen a clientes. Algunos desarrolladores se refieren a esta etapa como inspección previa (preview) o como una inspección previa técnica. Esta etapa comienza a menudo cuando los desarrolladores anuncian una congelación de las características del producto, indicando que no serán agregadas más características a esta versión y que solamente se harán pequeñas ediciones o se corregirán errores.

Las versiones beta están en un paso intermedio en el ciclo de desarrollo completo. Los desarrolladores las lanzan a un grupo de **probadores beta** o betatesters (a veces el público en general) para una prueba de usuario. Los probadores divulgan cualquier error que encuentran y características, a veces de menor importancia, que quisieran ver en la versión final.

Cuando una versión beta llega a estar disponible para el público en general, a menudo es utilizada extensamente por los tecnológicamente expertos o familiarizados con versiones anteriores, como si el producto estuviera acabado.

VERSIÓN CANDIDATA A DEFINITIVA (RC)

Una versión **candidata a definitiva** o **candidata para el lanzamiento**, aunque más conocida por su nombre en inglés ***release candidate***, comprende un producto final, preparado para publicarse como versión definitiva a menos que aparezcan errores que lo impidan. En esta fase el producto implementa todas las funciones del diseño y se encuentra libre de cualquier error que suponga un punto muerto en el desarrollo. Muchas empresas de desarrollo utilizan frecuentemente este término. Otros términos relacionados incluyen gamma, delta (y tal vez más letras griegas) para versiones que están prácticamente completas pero todavía en pruebas; y omega para versiones que se creen libres de errores y se hallan en el proceso final de pruebas. Gamma, delta y omega son, respectivamente, la tercera, cuarta y última letras del alfabeto griego.

VERSIÓN DE DISPONIBILIDAD GENERAL (RTM)

La versión de disponibilidad general (también llamada "dorada") de un producto es su versión final. Normalmente es casi idéntica a la versión candidata final, con sólo correcciones de último momento. Esta versión es considerada muy estable y relativamente libre de errores con una calidad adecuada para una distribución amplia y usada por usuarios finales. En versiones comerciales, puede estar también firmada (usado para que los usuarios finales verifiquen que el código no ha sido cambiado desde su salida.

La expresión de que un producto "se ha dorado" significa que el código ha sido completado y que "está siendo producido masivamente y estará en venta próximamente".

2.2. SOFTWARE LIBRE

DEFINICIÓN:

El Software Libre es una especie particular de software, el mismo que nos permite cuatro libertades básicas:

1. **Ejecutarlo con cualquier propósito**
2. **Estudiar cómo funciona y adaptarlo a sus necesidades**
3. **Distribuir copias**
4. **Mejorarlo, y liberar esas mejoras al publico**

Con la única **restricción** del copyleft (o sea, cualquiera que redistribuya el software, con o sin cambios, debe dar las mismas libertades que antes), y con el **requisito** de permitir el acceso al código fuente (imprescindible para ejercer las libertades 1 y 3)

Ubicación del Software Libre en las distintas clasificaciones

1. **De acuerdo al costo de adquisición:** el Software Libre se puede presentar: de costo cero o de costo mayor que cero. Lo que lo diferencia del Software Propietario es que su costo es independiente del número de computadoras que se poseen.

2. **De acuerdo a la apertura del código fuente**: el Software Libre siempre es de código fuente abierto (open source), El ser "open source" implica una serie de ventajas que serán descriptas en las Ventajas del Software Libre.

3. **De acuerdo a su protección:** el Software Libre siempre está protegido con licencias, y más específicamente, con licencias de copyleft. ¿Por qué no de dominio público? Porque de ese modo cualquiera puede adueñarse de él, por ejemplo, adquiere un Software Libre, lo modifica, lo compila y lo distribuye con código cerrado. ¿Por qué no con Copyright?

Porque de esa manera alguien le puede agregar alguna restricción, por lo tanto no va a seguir siendo Software Libre.

4. **De acuerdo a su legalidad:** el Software Libre siempre es legal, porque al usarlo, estudiarlo, modificarlo, adaptarlo y/o mejorarlo no estoy violando ninguna norma, ya que de por si este tipo de software me permite hacerlo, con la única salvedad de no poder agregarle ninguna restricción adicional cuando lo transfiera a otra persona.

2.2.1. Libertades básicas del Software Libre

Libertad Cero: "usar el programa con cualquier propósito". Es decir, el ejercicio de esta libertad implica que lo podemos utilizar con cualquier fin, ya sea educativo, cultural, comercial, político, social, etc. Esta libertad deriva de que hay ciertas licencias que restringen el uso del software a un determinado propósito, o que prohíben su uso para determinadas actividades.

Libertad Uno: "Estudiar cómo funciona el programa, y adaptarlo a sus necesidades". Significa que podemos **estudiar su funcionamiento** (al tener acceso al código fuente) lo que nos va a permitir, entre otras cosas: descubrir funciones ocultas, averiguar cómo realiza determinada tarea, descubrir que otras posibilidades tiene, que es lo que le falta para hacer algo, etc. El **adaptar el programa a nuestras necesidades** implica que podemos suprimirle partes que no nos interesan, agregarle partes que consideramos importantes, copiarle una parte que realiza una tarea y adicionarla a otro programa, etc.

Libertad Dos: "Distribuir copias". Quiere decir que soy libre de redistribuir el programa, ya sea gratis o con algún costo, ya sea por email, FTP o en CD, ya sea a una persona o a varias, ya sea a un vecino o a una persona que vive en otro país, etc.

Libertad Tres: "Mejorar el programa, y liberar las mejoras al público". Tengo la libertad de **hacer mejor el programa**, o sea que puedo: hacer menores los

requerimientos de hardware para funcionar, que tenga mayores prestaciones, que ocupe menos espacio, que tenga menos errores, etc.

El poder **liberar las mejoras al público** quiere decir que si yo le realizo una mejora que permita un requerimiento menor de hardware, o que haga que ocupe menos espacio, soy libre de poder redistribuir ese programa mejorado, o simplemente proponer la mejora en un lugar público (un foro de noticias, una lista de correo, un sitio Web, un FTP, un canal de Chat).

2.2.2. Ventajas del Software Libre

1. **Escrutinio Público:**

   Al ser muchos las personas que tienen acceso al código fuente, eso lleva a un proceso de corrección de errores muy dinámico, no hace falta esperar que el proveedor del software saque una nueva versión.

2. **Independencia del proveedor:**

   Software de dominio público: este tipo de software no tienen licencias de uso, por lo tanto corre el peligro de dejar de serlo si alguien lo utiliza con el fin de apropiárselo.

   - Al disponer del código fuente, cualquier persona puede continuar ofreciendo soporte, desarrollo u otro tipo de servicios para el software.
   - No estamos supeditados a las condiciones del mercado de nuestro proveedor, es decir que si este se va del mercado porque no le conviene y discontinua el soporte, nosotros podemos contratar a otra persona.

3. **Manejo de la Lengua:**

- Traducción: cualquier persona capacitada puede traducir y adaptar un

software libre a cualquier lengua.

- Corrección ortográfica y gramatical: una vez traducido el software libre puede presentar errores de este tipo, los cuales pueden ser subsanados con mayor rapidez por una persona capacitada.

4. Mayor seguridad y privacidad:

Los sistemas de almacenamiento y recuperación de la información son públicos. Cualquier persona puede ver y entender cómo se almacenan los datos en un determinado formato o sistema.
Existe una mayor dificultad para introducir código malicioso como ser: espía (p/ej. capturador de teclas), de control remoto (p/ej. Troyano), de entrada al sistema (p/ej. puerta trasera), etc.

5. **Garantía de continuidad:**

El software libre puede seguir siendo usado aun después de que haya desaparecido la persona que lo elaboro, dado que cualquier técnico informático puede continuar desarrollándolo, mejorándolo o adaptándolo.

6. **Ahorro en costos:**

En cuanto a este tópico debemos distinguir cuatro grandes costos: de adquisición, de implantación (este a su vez se compone de costos de migración y de instalación), de soporte o mantenimiento, y de interoperabilidad. El software libre principalmente disminuye el costo de adquisición ya que al otorgar la libertad de distribuir copias la puedo ejercer con la compra de una sola licencia y no con tantas como computadoras posea (como sucede en la mayoría de los casos de software propietario). Cabe aclarar que también hay una disminución significativa en el costo de soporte, no ocurriendo lo mismo con los costos de implantación y de interoperabilidad.

2.2.3. DESVENTAJAS DEL SOFTWARE LIBRE

Si observamos la situación actual, es decir la existencia mayoritaria de Software Propietario, tenemos:

a) **Dificultad en el intercambio de archivos:** esto se da mayormente en los documentos de texto (generalmente creados con Microsoft Word), ya que si los queremos abrir con un Software Libre, nos da error o se pierden datos. Pero está claro que si Microsoft Word creara sus documentos con un formato abierto (o público) esto no sucedería.

b) **Mayores costos de implantación e interoperabilidad:** ya que el software constituye "algo nuevo", ello supone afrontar un costo de aprendizaje, de instalación, de migración, de interoperabilidad, etc., cuya cuantía puede verse disminuida por: facilidad en las instalaciones y/o en el uso, uso de emuladores, vale aclarar que el costo de migración está referido al software, ya que en lo que hace a Hardware generalmente el Software Libre no posee mayores requerimientos que el Software Propietario.

2.2.4. Maneras de obtener software libre

a. **A través de copias en CD:** los que a su vez se pueden conseguir en revistas especializadas, o comprándolos en una casa de computación, o pidiéndoselos a un amigo, pariente, etc.

b. **A través de Internet:** a su vez, por medio de FTP, sitios Web, canales de chat, foros de noticias, programas de intercambio de archivos, etc.

c. A través de una computadora: en este caso, comprando una que venga con Software Libre pre instalado, ya sea de fábrica o por su vendedor. [5]

[5] http://www.monografias.com/trabajos12/elsoflib/elsoflib.shtml

2.3. NORMAS ISO

La **Organización Internacional para la Estandarización** o **ISO** Nacida tras la Segunda Guerra Mundial (23 de febrero de 1947), es el organismo encargado de promover el desarrollo de normas internacionales de fabricación, comercio y comunicación para todas las ramas industriales a excepción de la eléctrica y la electrónica. Su función principal es la de buscar la estandarización de normas de productos y seguridad para las empresas u organizaciones a nivel internacional.

La ISO es una red de los institutos de normas nacionales de 163 países, sobre la base de un miembro por país, con una Secretaría Central en Ginebra (Suiza) que coordina el sistema. La Organización Internacional de Normalización (ISO), con sede en Ginebra, está compuesta por delegaciones gubernamentales y no gubernamentales subdivididos en una serie de subcomités encargados de desarrollar las guías que contribuirán al mejoramiento ambiental.

Las normas desarrolladas por ISO son voluntarias, comprendiendo que ISO es un organismo no gubernamental y no depende de ningún otro organismo internacional, por lo tanto, no tiene autoridad para imponer sus normas a ningún país. El contenido de los estándares está protegido por derechos de copyrigh y para acceder ellos el público corriente debe comprar cada documento, que se valoran en francos suizos.

Está compuesta por representantes de los organismos de normalización (ON) nacionales, que produce normas internacionales industriales y comerciales.

Dichas normas se conocen como *normas ISO* y su finalidad es la coordinación de las normas nacionales, en consonancia con el Acta Final de la Organización Mundial del Comercio, con el propósito de facilitar el comercio, el intercambio de información y contribuir con normas comunes al desarrollo y a la transferencia de tecnologías.

2.3.1. ¿Qué es una Norma?

Las normas son un modelo, un patrón, ejemplo o criterio a seguir. Una norma es una fórmula que tiene valor de regla y tiene por finalidad definir las características que debe poseer un objeto y los productos que han de tener una compatibilidad para ser usados a nivel internacional. Pongamos, por ejemplo, el problema que ocasiona a muchos usuarios los distintos modelos de enchufes que existen a escala internacional para poder acoplar pequeñas máquinas de uso personal: secadores de cabello, máquinas de afeitar, etc., cuando se viaja. La incompatibilidad repercute en muchos campos. La normalización de los productos es, pues, importante.[6]

2.3.2. ¿Qué son las normas ISO?

Las normas ISO surgen para armonizar la gran cantidad de normas sobre gestión de calidad que estaban apareciendo en distintos países del mundo.

Los organismos de normalización de cada país producen normas que resultan del consenso entre representantes del estado y de la industria. De la misma manera las normas ISO surgen del consenso entre representantes de los distintos países integrados a la I.S.O.

Existen dos grandes familias de normas ISO:
Las de la familia 9000 y las de la familia 14000 además de otras complementarias (ISO 8402; ISO 10011).

La finalidad principal de las normas ISO es orientar, coordinar, simplificar y unificar los usos para conseguir menores costes y efectividad.

Tiene valor indicativo y de guía. Actualmente su uso se va extendiendo y hay un gran interés en seguir las normas existentes porque desde el punto de vista económico reduce costes, tiempo y trabajo. Criterios de eficacia y de

[6] http://www.ub.es/geocrit/b3w-129.htm

capacidad de respuesta a los cambios. Por eso, las normas que presentemos, del campo de la información y documentación, son de gran utilidad porque dan respuesta al reto de las nuevas tecnologías.[7]

2.4. GESTIÓN DE LA CALIDAD

Se llama gestión de la calidad al aspecto de la función general de la empresa que determina y aplica la política de la calidad. La obtención de la calidad deseada requiere el compromiso y la participación de todos los miembros de la empresa, la responsabilidad de la gestión recae en la alta dirección de la empresa. Esta gestión incluye planificación, organización y control del desarrollo del sistema y otras actividades relacionadas con la calidad, la implantación de la política de calidad de una empresa requiere un sistema de la calidad, entendiendo como tal el conjunto de estructura, organización, responsabilidades, procesos, procedimientos y recursos que se establecen para llevar a cabo la gestión de la calidad. El sistema de la calidad no deberá extenderse más que a las exigencias para realizar los objetivos de la calidad.

¿Qué entendemos por calidad?

La calidad es la estructura ósea de una organización; Las finanzas son su nutrición; y las relaciones son el espíritu.

La Calidad está controlada por el cliente, esto quiere decir que el cliente determina qué es exactamente la calidad, y nadie más puede hacerlo.

Muchas organizaciones piensan que pueden imponer la calidad al cliente, pero luego descubren que no es así.

Los clientes deben decidir lo que quieren y la labor de una organización es escucharlos y después obedecer. [8]

[7] http://www.promer.org/getdoc.php?docid=87
[8] Philip B. Crosby, Completeness (Plenitud), Calidad para el siglo XXI, Cap: 10

2.4.1. SISTEMA DE GESTIÓN DE LA CALIDAD

Un **sistema de gestión de la calidad** es el conjunto de normas interrelacionadas de una empresa u organización por los cuales se administra de forma ordenada la calidad de la misma, en la búsqueda de la satisfacción de las necesidades y expectativas de sus clientes. Entre dichos elementos, los principales son:

1. Estructura de la organización: responde al organigrama de los sistemas de la empresa donde se jerarquizan los niveles directivos y de gestión. En ocasiones este organigrama de sistemas no corresponde al organigrama tradicional de una empresa.

2. Estructura de responsabilidades: implica a personas y departamentos. La forma más sencilla de explicitar las responsabilidades en calidad, es mediante un cuadro de doble entrada, donde mediante un eje se sitúan los diferentes departamentos y en el otro, las diversas funciones de la calidad.

3. Procedimientos: responden al plan permanente de pautas detalladas para controlar las acciones de la organización.

4. Procesos: responden a la sucesión completa de operaciones dirigidos a la consecución de un objetivo específico.

5. Recursos: no solamente económicos, sino humanos, técnicos y de otro tipo, deben estar definidos de forma estable y circunstancial.

Estos cinco apartados no siempre están definidos ni son claros en una empresa.

Implementación

Existen diversos métodos para la implementación de los sistemas de gestión

de la calidad y siempre se requiere usar herramientas propias, sin embargo, para poder ser aplicable es preciso tomar en cuenta el contexto laboral, sociocultural y político, ya que éstas dimensiones determinará el enfoque gerencial para la calidad de la organización. La implementación de un excelente sistema de calidad ayudara a la organización a cumplir con los requisitos de sus clientes en cuanto al producto y a la prestación del servicio que ofrece a sus clientes y generar en ellos satisfacción.

2.4.2. GESTIÓN DE CALIDAD POR PROCESOS

Objetivos

- Conocer la metodología de la gestión por procesos
- Conocer cómo diseñar procesos

PROCESO Es el "conjunto de actuaciones, decisiones, actividades y tareas que se encadenan de forma secuencial y ordenada para conseguir un resultado que satisfaga plenamente los requerimientos del cliente al que va dirigido".

En otras palabras, un proceso no es más que la sucesión de pasos y decisiones que se siguen para realizar una determinada actividad o tarea que, cuando se trabaja desde el enfoque de la Calidad Total, deben ir orientados a satisfacer a nuestro cliente

Definimos proceso como "el conjunto de actividades secuenciales que realizan una transformación de una serie de inputs (material, mano de obra, capital, información, etc.) en los outputs deseados (bienes y/o servicios) añadiendo valor**".**

La gestión por procesos busca reducir la variabilidad innecesaria que aparece habitualmente cuando se producen o prestan determinados servicios y trata de eliminar las ineficiencias asociadas a la repetitividad de las acciones o actividades, al consumo inapropiado de recursos, etc. Todo proceso incluye una sucesión de actividades que, necesariamente, tienen cada una de ellas alguna actividad precedente y lógicamente tendrán otra a continuación hasta

su final. Al espacio entre los límites establecidos para cada proceso, se le denomina ámbito del proceso.

En el caso concreto de las empresas del sector servicios, donde coincide que el producto se consume en el momento en el que se produce, se actúa sobre el propio cliente al que se considera como “sustrato” (entrada) a transformar en producto con valor añadido al término del proceso de prestación de un servicio (salida). Por ello, el producto obtenido en el sector servicios se fundamenta en el mismo cliente, al que se ha aportado el valor añadido con una prestación de servicio determinada.

Para utilizar la gestión por procesos en una organización, debe describirse de forma clara su misión (en qué consiste, para qué existe y para quién se realiza), concretando, a continuación, entradas y salidas e identificando clientes y proveedores del mismo. Se debe poder medir la cantidad y la calidad de lo producido, el tiempo desde la entrada hasta la salida y el coste invertido en añadir valor; y, por último, ha de poder asignarse la responsabilidad del cumplimiento de la misión del proceso a una persona (al que denominamos habitualmente propietario del proceso).

Un proceso se visualiza normalmente en forma de diagrama o esquema, que describe en forma gráfica el modo en que las personas desempeñan su trabajo. Estos diagramas o esquemas pueden aplicarse a cualquier secuencia de actividades que se repita y que pueda medirse, independientemente de la longitud de su ciclo o de su complejidad, aunque para que sea realmente útil debe permitir cierta sencillez y flexibilidad.

En las organizaciones se dan cita diferentes tipos de procesos:

- **Procesos clave**, los que representan la razón de ser de nuestra unidad o departamento, nuestro objeto principal de actividad, de los que fundamentalmente vamos a hablar aquí
- **Procesos de soporte** que tienen como misión apoyar a uno o más procesos clave

- Aquellos que **crean y gestionan infraestructuras** y posibilitan los anteriores
- Aquellos otros procesos **de gobierno** que orientan y dirigen todos los procesos, marcando la estrategia de la organización.

Una forma de representar gráficamente un proceso clave puede empezar por delimitar su “salida” su “entrada”, su marco estratégico y sus procesos de soporte.

Para describir un proceso se recomienda seguir este orden:

- Definirlo, especificar de qué se trata, sus límites y responsable. Definir su misión y objetivos.

- Identificar quién es el beneficiario (cliente) del proceso, describir sus expectativas y sus necesidades como “salidas” del proceso, e identificar los estándares de calidad aceptables para nuestros clientes.

- Relacionar las actividades que se incluyen en el proceso, sus elementos, diagrama, secuencia, “entradas” y requisitos de calidad

- Especificar el método de evaluación y de revisión que adoptaremos para introducir mejoras en el proceso, lo que incluye determinar indicadores del proceso.

¿Por qué la gestión por Procesos?

Por que las empresas y/o las organizaciones son tan eficientes como lo son sus procesos. La Mayoría de las empresas y las organizaciones que han tomado conciencia de esto han reaccionado ante la ineficiencia que representa las organizaciones departamentales, con sus nichos de poder y su inercia excesiva ante los cambios, potenciando el concepto del proceso, con un foco común y trabajando con una visión de objetivo en el cliente.

La Gestión por Procesos es la forma de gestionar toda la organización basándose en los Procesos. En tendiendo estos como una secuencia de actividades orientadas a generar un valor añadido sobre una ENTRADA para conseguir un resultado, y una SALIDA que a su vez satisfaga los requerimientos del Cliente.

SE HABLA REALMENTE DE PROCESO SI CUMPLE LAS SIGUIENTES CARACTERÍSTICAS O CONDICIONES

- Se pueden describir las ENTRADAS y las SALIDAS
- El Proceso cruza uno o varios límites organizativos funcionales.
- Una de las características significativas de los procesos es que son capaces de cruzar verticalmente y horizontalmente la organización.
- Se requiere hablar de metas y fines en vez de acciones y medios. Un proceso responde a la pregunta "QUE", no al "COMO".
- El proceso tiene que ser fácilmente comprendido por cualquier persona de la organización.
- El nombre asignado a cada proceso debe ser sugerente de los conceptos y actividades incluidos en el mismo.

2.4.2.1. CÍRCULO DE DEMING

El ciclo **PDCA**, también conocido como "Círculo de Deming" (de Edwards Deming), es una estrategia de mejora continua de la calidad en cuatro pasos, basada en un concepto ideado por Walter A. Shewhart. También se denomina *espiral de mejora continua*. Es muy utilizado por los SGC.

Las siglas **PDCA** son el acrónimo de **P**lan, **D**o, **C**heck, **A**ct (Planificar, Hacer, Verificar, Actuar).

PLAN (Planificar)

- Identificar el proceso que se quiere mejorar
- Recopilar datos para profundizar en el conocimiento del proceso
- Análisis e interpretación de los datos
- Establecer los objetivos de mejora
- Detallar las especificaciones de los resultados esperados
- Definir los procesos necesarios para conseguir estos objetivos, verificando las especificaciones

DO (Hacer)

- Ejecutar los procesos definidos en el paso anterior
- Documentar las acciones realizadas.

CHECK (Verificar)

- Pasado un periodo de tiempo previsto de antemano, volver a recopilar datos de control y analizarlos, comparándolos con los objetivos y especificaciones iniciales, para evaluar si se ha producido la mejora esperada
- Documentar las conclusiones

ACT (Actuar)

- Modificar los procesos según las conclusiones del paso anterior para alcanzar los objetivos con las especificaciones iniciales, si fuese necesario
- Aplicar nuevas mejoras, si se han detectado errores en el paso anterior
- Documentar el proceso

Todos los procesos tienen que ser capaces de satisfacer los ciclos P, D, C, A de la **figura 5** adjunta.

Todos los procesos tienen que tener indicadores que permitan visualizar de forma gráfica la evolución de los mismos. Tienen que ser planificados en la fase P, tienen que asegurarse su cumplimiento en la fase D, tienen que servir para realizar el seguimiento en la fase C y tiene que utilizarse en la fase A para ajustar y/o establecer objetivos.

Figura #5. Círculo de Deming

Fuente: http://www.sintelec.es/semaforo/html/caract.html

Es recomendable planificar y realizar periódicamente (Aproximadamente 3 años) una reingeniería de los procesos de gestión para alcanzar mejoras espectaculares en determinados parámetros como costes, calidad, servicio y rapidez de respuesta.

Una forma más moderna y completa de ver estos ciclos de revisión y mejora se

encuentra dentro de la filosofía REDER.

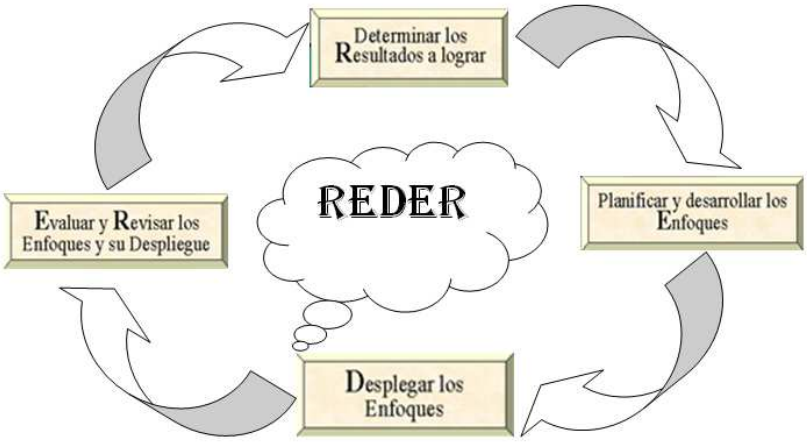


Figura #6. Filosofía REDER

Fuente: http://web.jet.es/amozarrain/Gestion_procesos.htm

2.4.2.2. MÉTODOS PARA LA IDENTIFICACIÓN DE PROCESOS

Aquí ya entramos en materia. Básicamente se puede asegurar que existen muchos métodos para la identificación de los procesos. Pero a mi entender se pueden englobar en dos grande**s grupos:**

Método "ESTRUCTURADO": En este apartado estoy englobando todos aquellos sistemas básicamente complejos que sirven para la identificación de los procesos de gestión. Estamos hablando de los sistemas informatizados.

Lo que tienen en común todos estos sistemas es que los mismos están diseñados por personas expertas. Normalmente su implantación requiere de algún tipo de asistencia externa.

Ventajas:

Son sistemas estructurados que sirven para identificar y documentar un proceso de gestión. Se dan pautas, guías, soportes y hasta plantillas.

Estos sistemas permiten identificar áreas de gestión que no se abordan y/o

ineficientes. Los procesos y subprocesos relacionados están perfectamente documentados.

Si se consigue mantener actualizada toda la documentación asociada a los mismos se convierten en herramientas validas para la formación de los nuevos ingresos. No olvidemos que esto de la gestión del conocimiento es una asignatura pendiente por mucho que se hable de la misma.

Inconvenientes:

Los procesos de gestión son demasiado documentados.

.

Otro de los problemas asociados a este tipo de sistemas es que normalmente no suelen saber qué hacer con los procedimientos existentes y sus sistemas relacionados. Me estoy refiriendo a los procedimientos y a los Sistemas de Calidad, Medio Ambiente y Prevención de Riesgos Laborales. De esta forma una empresa se encuentra con un nuevo Sistema de Procesos que no sabe muy bien relacionar con los otros sistemas existentes.

Método "CREATIVO": En este apartado se engloba todos aquellos métodos que las empresas están ideando e implantado de forma interna. Normalmente motivadas por las nefastas experiencias y/o por la ineficiencia del método anterior.

Ventajas:

El Sistema de Gestión está mucho más integrado, ya que tanto el método ideado como todos los soportes relacionados están creados internamente por miembros de la organización. Estos soportes y métodos se convierten con poco esfuerzo en documentos "entendibles" por el resto del personal.

La documentación se reduce drásticamente. Los procedimientos desaparecen y se "convierten" y/o se incorporan a los procesos relacionados.

Inconvenientes:

Se requiere de personas expertas en todos los campos citados. Es decir alguien que conozca el Sistema de Calidad, Medio Ambiente, Prevención Riesgos Laborales y Gestión de o por Procesos.

Se debe hacer más énfasis en la formación de las nuevas incorporaciones ya que buena parte del conocimiento no está ni en papel ni en soportes informáticos. Se tiene que fomentar la formación de "oído a oído".

Selección del método

La elección del método dependerá del conocimiento que tengan los miembros de la empresa en el cual se encuentre la misma. A groso modo y como orientación se puede ver algunas ideas relacionadas con cada uno de los métodos expuestos. En caso de dudas lo mejor es escoger el método estructurado y recurrir a una asesoría.

También podría ser una combinación de ambas. [9]

2.4.3. ¿Para qué la Gestión por Procesos?

- Mejora continua de las actividades desarrolladas
- Reducir la variabilidad innecesaria
- Eliminar las ineficiencias asociadas a la repetitividad de las actividades
- Optimizar el empleo de los recursos

Pasos para la Gestión por procesos

- Identificar clientes y sus necesidades
- Definir servicios/productos
- Desarrollar el mapa de procesos

[9] http://web.jet.es/amozarrain/Gestion_procesos.htm

- Describir procesos
- Diagramar procesos
- Análisis de datos y mejora del proceso

Definir la Misión

- Identifica el objetivo fundamental de la unidad, su razón de ser.

1. Identificar clientes y sus necesidades

- Objetivo organización:
    - Satisfacer las necesidades y expectativas de sus clientes
- Tipos clientes:
    - Internos
    - Externos

2. Definir productos/servicios

- Conociendo los clientes, se determina qué productos y/o servicios se les está ofreciendo.

3. Desarrollar el mapa de procesos

- **Procesos estratégicos**:

  Procesos que orientan y dirigen los procesos clave y de soporte

- **Procesos clave:**

  La razón de ser de nuestra empresa o unidad, el objetivo principal de actividad

- **Procesos de soporte:**
    - Los que apoyan a uno o más de nuestros **procesos** clave

2.4.4. Mapas de Procesos

A pesar de que en ISO no existe el requisito de desarrollar concretamente un mapa de procesos, si se ha convertido una práctica generalizada por las empresas certificadas o en proceso de certificación, probablemente siguiendo lo establecido en los requisitos generales del apartado 4.1 de la Norma ISO 9001:2008 que establece que la organización debe a) identificar los procesos necesarios para el sistema de gestión de la calidad y su aplicación a través de la organización y b) determinar la secuencia e interacción de estos procesos.

Los mapas de procesos tienen su origen en la utilización de los mapas mentales, los cuales presentan de una forma lógica y clara temas complejos. [10]

Los mapas mentales han sido utilizados, sobre todo en procesos de enseñanza - aprendizaje, ya que permite obtener mejores resultados en distintos aspectos de la vida laboral y personal.

El diseño de un mapa mental es útil para organizar información, administrar el tiempo, liderar gente, o alinear objetivos y estrategias. Los mapas mentales constituyen un método para plasmar sobre el papel el proceso natural del pensamiento.

Tanto el mapa de procesos como el mapa estratégico debería ser una representación gráfica de cómo la empresa espera alcanzar los resultados planificados para el logro de su estrategia o política de calidad. Algunos de los mapas de procesos analizados, en muchos casos, reflejan una descripción de los requisitos de la normativa en lugar de presentar como la empresa ha planificado alcanzar los resultados.

En otros casos es una descripción de la interacción de procesos, parecido a una distribución de planta, otros asemejan organigramas funcionales. Por su

[10] http://www.upm.es/innovacion/calidad/documentos/Gestion_Procesos.ppt.

parte algunos de los mapas estratégicos, presentan un conjunto de objetivos o elementos estratégicos en las cuatro perspectivas, que no tienen ninguna relación entre sí o bien no se determina con claridad la relación causa efecto.[11]

2.4.5. NORMA ISO 9001

Es un conjunto de normas sobre la calidad y la gestión. La **Norma ISO 9001** ha sido elaborada por el Comité Técnico ISO/TC176 de ISO Organización Internacional para la Estandarización y especifica los requisitos para un buen sistema de gestión de la calidad que pueden utilizarse para su aplicación interna por las organizaciones, para certificación o con fines contractuales.

La norma ISO 9001 tiene origen en la norma BS 5750, publicada en 1979 por la entidad de normalización británica, la [British Standards Institution] (BSI).

La versión actual de ISO 9001 (la cuarta) data de noviembre de 2008, y por ello se expresa como ISO 9001:2008. Versiones ISO 9001 hasta la fecha:

- Cuarta versión: la actual ISO 9001:2008 (15/11/2008)
- Tercera versión: ISO 9001:2000 (15/12/2000)
- Segunda versión: ISO 9001:94 - ISO 9002:94 - ISO 9003:94 (01/07/1994)
- Primera versión: ISO 9001:87 - ISO 9002:87 - ISO 9003:87 (15/03/1987)

En la primera y segunda versión de ISO 9001, la Norma se descomponía en 3 normas: ISO 9001, ISO 9002, e ISO 9003.

- ISO 9001 --> organizaciones con diseño de producto
- ISO 9002 --> organizaciones sin diseño de producto pero con producción/fabricación.

[11] http://www.monografias.com/trabajos16/mapas-proceso-estrategicos/mapas-proceso-estrategicos.shtml

- ISO 9003 --> organizaciones sin diseño de producto ni producción/fabricación (comerciales).

El contenido de las 3 normas era el mismo, con la excepción de que en cada caso se excluían los requisitos de aquello que no aplicaba. Esta mecánica se modificó en la tercera versión, unificando los 3 documentos en un único estándar, sobre el cual se realizan posteriormente las exclusiones.

La cuarta versión de la norma presenta más de 60 modificaciones que se reparten de la siguiente forma.

Descripción

Toda organización puede mejorar su manera de trabajar, lo cual significa un incremento de sus clientes y gestionar el riesgo de la mejor manera posible, reduciendo costes y mejorando la calidad del servicio ofrecido. La gestión de un sistema de calidad aporta el marco que se necesita para supervisar y mejorar la producción en el trabajo. Con mucha diferencia, en cuanto a calidad se refiere, la normativa más establecida y conocida es la ISO 9001, la cual establece una norma no sólo para la Gestión de Sistemas de Calidad sino para cualquier sistema en general. La ISO 9001 está ayudando a todo tipo de organizaciones a tener éxito, a través de un incremento de la satisfacción del cliente y de la motivación del departamento.

La ISO 9001:2008 es **válida para cualquier organización**, independientemente de su tamaño o sector, que busque mejorar la manera en que se trabaja y funciona. Además, los mejores retornos en la inversión, vienen de compañías preparadas para implantar la citada normativa en cualquier parte de su organización.

Estructura de ISO 9001:2008

La norma ISO 9001:2008 está estructurada en ocho capítulos, refiriéndose los TRES primeros a declaraciones de principios, estructura y descripción de la empresa, requisitos generales, etc., es decir, son de carácter introductorio. Los

capítulos CUATRO a OCHO están orientados a procesos y en ellos se agrupan los requisitos para la implantación del sistema de calidad.

A la fecha, ha habido cambios en aspectos claves de la norma ISO 9001, al 15 de noviembre del 2008, la norma 9001 varía.

Los ocho capítulos de ISO 9001 son:

1. Guías y descripciones generales, no se enuncia ningún requisito.
    1. Generalidades.
    2. Reducción en el alcance.
2. Normativas de referencia.
3. Términos y definiciones.
4. **Sistema de gestión**: contiene los requisitos generales y los requisitos para gestionar la documentación.
    1. Requisitos generales.
    2. Requisitos de documentación.
5. **Responsabilidades de la Dirección**: contiene los requisitos que debe cumplir la dirección de la organización, tales como definir la política, asegurar que las responsabilidades y autoridades están definidas, aprobar objetivos, el compromiso de la dirección con la calidad, etc.
    1. Requisitos generales.
    2. Requisitos del cliente.
    3. Política de calidad.
    4. Planeación.
    5. Responsabilidad, autoridad y comunicación.
    6. Revisión gerencial.
6. **Gestión de los recursos**: la Norma distingue 3 tipos de recursos sobre los cuales se debe actuar: RRHH, infraestructura, y ambiente de trabajo. Aquí se contienen los requisitos exigidos en su gestión.
    1. Requisitos generales.
    2. Recursos humanos.
    3. Infraestructura.
    4. Ambiente de trabajo.

7. **Realización del producto**: aquí están contenidos los requisitos puramente productivos, desde la atención al cliente, hasta la entrega del producto o el servicio.
    1. Planeación de la realización del producto y/o servicio.
    2. Procesos relacionados con el cliente.
    3. Diseño y desarrollo.
    4. Compras.
    5. Operaciones de producción y servicio
    6. Control de equipos de medición, inspección y monitoreo
8. **Medición, análisis y mejora**: aquí se sitúan los requisitos para los procesos que recopilan información, la analizan, y que actúan en consecuencia. El objetivo es mejorar continuamente la capacidad de la organización para suministrar productos que cumplan los requisitos.(pero nadie lo toma en serio (eso es muy generalizado)) El objetivo declarado en la Norma, es que la organización busque sin descanso la satisfacción del cliente a través del cumplimiento de los requisitos.
    1. Requisitos generales.
    2. Seguimiento y medición.
    3. Control de producto no conforme.
    4. Análisis de los datos para mejorar el desempeño.
    5. Mejora.

ISO 9001:2008 tiene muchas semejanzas con el famoso “Círculo de Deming o PDCA”; Está estructurada en cuatro grandes bloques, completamente lógicos, y esto significa que con el modelo de sistema de gestión de calidad basado en ISO se puede desarrollar en su seno cualquier actividad. La ISO 9000:2008 se va a presentar con una estructura válida para diseñar e implantar cualquier sistema de gestión, no solo el de calidad, e incluso, para integrar diferentes sistemas.

ISO 9001 forma parte de la Familia de Normas ISO 9000:

Ventaja competitiva

Según la ISO 9001, debería ser la Dirección General la que se asegure de que los directores de los distintos departamentos se están acercando a un sistema de gestión. Nuestra evaluación y el proceso de certificación aseguran que los objetivos del negocio se alimentan del sistema día a día, favoreciendo las mejores prácticas de los trabajadores y de los procesos.

Mejora del funcionamiento del negocio y gestión del riesgo

La ISO 9001 ayuda a sus gerentes a mejorar el funcionamiento de la organización y a diferenciarse de aquellos competidores que no usan el sistema. La certificación también hace más fácil medir el funcionamiento y gestionar los posibles riesgos.

Atrae la inversión, realza la reputación de marca y elimina las barreras al comercio

La certificación ISO 9001 mejorará su reputación de marca y puede ser utilizada como una herramienta de marketing. Manda un mensaje claro a todos los accionistas de que la compañía está comprometida con las normas y la mejora continua.

Ahorro de costes

La experiencia nos enseña que los beneficios financieros de las compañías que han invertido en un sistema de gestión de calidad ISO 9001 han sido los siguientes: una mayor eficiencia operacional, incrementando sus ventas, con un retorno en la inversión de los activos y una mayor rentabilidad.

Mejora la operación y reduce gastos

La auditoría del sistema de gestión de calidad está focalizada en el proceso operativo. Esto anima a las organizaciones a mejorar la calidad de los productos y de los servicios prestados, ayuda a reducir el gasto, así como las devoluciones y reclamaciones de los clientes.

Aumenta la comunicación interna y eleva la moral

La ISO 9001 permite que los empleados se sientan más involucrados a través de una mejora en las comunicaciones. Las visitas de evaluación continua pueden destacar cualquier deficiencia en las habilidades de los empleados y destacar cualquier problema en el desarrollo del trabajo en equipo.

Incrementa la satisfacción del cliente

La estructura “planear, realizar, revisar y actuar” PDCA de la ISO 9001 asegura que las necesidades de los clientes van a seguir siendo consideradas y conocidas[12]

2.4.6. CASOS DE ÉXITO DE IMPLANTACIÓN DE NORMA ISO 9001

1.- Navarcable

Figura # 7. Logo de Navarcable.

Fuente: http://www.navarcable.com

Origen: España

Fecha de Implementación: 15-03-2008

Navarcable revoluciona su gestión empresarial

"Optimizar los procesos de fabricación a partir de una exhaustiva clasificación de productos y manejar una gran cantidad de ofertas y pedidos eran los objetivos prioritarios."

Desde su fundación en 2001, la preocupación de esta firma por la calidad ha sido máxima.

[12] http://es.wikipedia.org/wiki/Normas_ISO_9000

Así esta organización ha implantado un sistema de gestión de calidad basado en la normas ISO 9001.

Actualmente, El volumen de ventas que maneja Navarcable, está aumentando de manera considerable y se prevé un proceso de expansión internacional.

Para mayor información del proceso de éxito de Navarcable, viste la página: http://www.tipsa.net/downloads/casos/navarcable.pdf

2.- PiN Producción Informática

Figura # 8. Logo PiN Producción Informática.

Fuente: http://www.pinsl.es

Origen: España

Fecha de Implementación: 01-2010

En PINSL nos planteamos el objetivo ambicioso e innovador de ser pioneros en la certificación internacional de un Sistema Integrado que abarcase el aseguramiento de la Calidad (ISO 9001), en todos nuestros sistemas presentes y futuros.

Es por esta razón que desde la implantación de nuestro SGC PINSL ha mejorado en los siguientes aspectos:

- Las áreas en general están más ordenadas
- El personal trabaja con enfoque de satisfacción al cliente.
- Se es más competitivo, más seguro.
- Se establece la mejora continua, como método de trabajo.
- Mayor satisfacción de los grupos de interés (personal interno, clientes, proveedores, sociedad).

- La implicación de todas las áreas de la Empresa está unificada y es más sólida.
- Se genera el “orgullo corporativo” del personal interno.

Para mayor información del proceso de éxito de PINSL, visite la página:

http://www.aslan.es/files/1149-21496-Archivo/certificacionnavarra.pdf

2.5. SEGURIDAD DE LA INFORMACIÓN

Se entiende por seguridad de la información a todas aquellas medidas preventivas y reactivas del hombre, de las organizaciones y de los sistema tecnológicos que permitan resguardar y proteger la información buscando mantener la *confidencialidad*, la *autenticidad* y *Integridad* de la misma.

El concepto de seguridad de la información no debe ser confundido con el de seguridad informática, ya que este último sólo se encarga de la seguridad en el medio informático, pudiendo encontrar información en diferentes medios o formas.

Para el hombre como individuo, la seguridad de la información tiene un efecto significativo respecto a su privacidad, la que puede cobrar distintas dimensiones dependiendo de la cultura del mismo.

El campo de la seguridad de la información ha crecido y evolucionado considerablemente a partir de la Segunda Guerra Mundial, convirtiéndose en una carrera acreditada a nivel mundial.

Historia de la seguridad de la información

Desde tiempos inmemorables el hombre ha resguardado y protegido con celo sus conocimientos debido a la ventaja y poder que éste le producía sobre otros hombres o sociedades.

En la antigüedad surgen las bibliotecas, lugares donde se podía resguardar la

información para trasmitirla y para evitar que otros la obtuvieran, dando así algunas de las primeras muestras de protección de la información.

Sun Tzu en El arte de la guerra y Nicolás Maquiavelo en El Príncipe señalan la importancia de la información sobre los adversarios y el cabal conocimiento de sus propósitos para la toma de decisiones.

Durante la Segunda Guerra Mundial se crean la mayoría de los servicios de inteligencia del mundo con el fin de obtener información valiosa e influyente, creándose grandes redes de espionaje. Como forma de protección surge la contrainteligencia.

Con el devenir de los años al incrementarse el alcance de la tecnología, el cuidado de la información se ha vuelto crucial para los hombres, las organizaciones y las sociedades.

Concepción de la seguridad de la información

En la seguridad de la información es importante señalar que su manejo está basado en la tecnología y debemos de saber que puede ser confidencial: la información está centralizada y puede tener un alto valor. Puede ser divulgada, mal utilizada, ser robada, borrada o saboteada. Esto afecta su disponibilidad y la pone en riesgo.

La información es poder y a la información se le conoce como:

Critica: Es indispensable para la operación de la empresa.
Valiosa: Es un activo de la empresa y muy valioso.
Sensitiva: Debe de ser conocida por las personas autorizadas

Existen dos palabras muy importantes que son riesgo y seguridad:

Riesgo: Es todo tipo de vulnerabilidades, amenazas que pueden ocurrir sin previo aviso y producir numerosas pérdidas para las empresas. Los riesgos

más perjudiciales son a las tecnologías de información y comunicaciones.

Seguridad: Es una forma de protección contra los riesgos

La seguridad de la información abarca muchas cosas, pero todas estas giran en torno a la información. Por ejemplo la disponibilidad, comunicación, identificación de problemas, análisis de riesgos, la integridad, confidencialidad, recuperación de los riesgos.

Precisamente los riesgos es uno de los mayores problemas en la seguridad, ya que de TI debe de tener tres planos uno en el peor de los casos, otro un estado medio y un estado favorable. Ya que de esta manera se podrá mitigar el daño que se pueda provocar por que ya se tomaron medidas. No se puede decir que la seguridad teda un 100% de tranquilidad ya que cada día aparece un código nuevo o un ataque diferente, etc. pero tienes menos conflictos y un sistema en condiciones de producir.

Seguridad de la Información tiene como fin la protección de la información y de los sistemas de la información del acceso, uso, divulgación, interrupción o destrucción no autorizada.

El termino Seguridad de Información, Seguridad informática y garantía de la información son usados con frecuencia y aunque su significado no es el mismo, persiguen una misma finalidad al proteger la Confidencialidad, Integridad y Disponibilidad de la información; sin embargo, entre ellos existen algunas diferencias sutiles. Estas diferencias radican principalmente en el enfoque, las metodologías utilizadas, y las zonas de concentración.

La Seguridad de la Información se refiere a la Confidencialidad, Integridad y Disponibilidad de la información y datos, independientemente de la forma los datos pueden tener: electrónicos, impresos, audio u otras formas.

Además, la seguridad de la información involucra la implementación de estrategias que cubran los procesos en donde la información es el activo

primordial. Estas estrategias deben tener como punto primordial el establecimiento de políticas, controles de seguridad, tecnologías y procedimientos para detectar amenazas que puedan explotar vulnerabilidades y que pongan en riesgo dicho activo, es decir, que ayuden a proteger y salvaguardar tanto información como los sistemas que la almacenan y administran.

Cabe mencionar que la seguridad es un proceso continuo de mejora por lo que las políticas y controles establecidos para la protección de la información deberán revisarse y adecuarse, de ser necesario, ante los nuevos riesgos que surjan, a fin de tomar las acciones que permitan reducirlos y en el mejor de los casos eliminarlos.

Los Gobiernos, entidades militares, instituciones financieras, los hospitales y las empresas privadas de información confidencial sobre sus empleados, clientes, productos, investigación y su situación financiera. La mayor parte de esta información es recolectada, tratada, almacenada y puesta a la disposición de sus usuarios, en computadoras y trasmitida a través de las redes entre los ordenadores.

En caso de que la información confidencial de una empresa, sus clientes, sus decisiones, su estado financiero o nueva línea de productos caigan en manos de un competidor; se vuelva pública de forma no autorizada, podría ser causa de la pérdida de credibilidad de los clientes, pérdida de negocios, demandas legales o incluso la quiebra de la misma.

Por lo que proteger la información confidencial es un requisito del negocio, y en muchos casos también un imperativo ético y una obligación legal. .
Por más de veinte años la Seguridad de la Información ha declarado que la confidencialidad, integridad y disponibilidad (conocida como la Tríada CIA, del inglés: "Confidentiality, Integrity, Availability") son los principios básicos de la seguridad de la información.

La correcta Gestión de la Seguridad de la Información busca establecer y

mantener programas, controles y políticas, que tengan como finalidad conservar la confidencialidad, integridad y disponibilidad de la información, si alguna de estas características falla no estamos ante nada seguro. Es preciso anotar, además, que la seguridad no es ningún hito, es más bien un proceso continuo que hay que gestionar conociendo siempre las vulnerabilidades y las amenazas que se ciñen sobre cualquier información, teniendo siempre en cuenta las causas de riesgo y la probabilidad de que ocurran, así como el impacto que puede tener. Una vez conocidos todos estos puntos, y nunca antes, deberán tomarse las medidas de seguridad oportunas.

2.5.1. Objetivos de la seguridad de la Información

Generalmente, los sistemas de información incluyen todos los datos de una compañía y también en el material y los recursos de software que permiten a una compañía almacenar y hacer circular estos datos. Los sistemas de información son fundamentales para las compañías y deben ser protegidos.

Generalmente, la seguridad de la información consiste en garantizar que el material y los recursos de software de una organización se usen únicamente para los propósitos para los que fueron creados y dentro del marco previsto.

La seguridad de la información se resume, por lo general, en los siguientes objetivos principales:

Confidencialidad

La confidencialidad es la propiedad de prevenir la divulgación de información a personas o sistemas no autorizados.

Por ejemplo, una transacción de tarjeta de crédito en Internet requiere que el número de tarjeta de crédito a ser transmitida desde el comprador al comerciante y el comerciante de a una red de procesamiento de transacciones.

El sistema intenta hacer valer la confidencialidad mediante el cifrado del

número de la tarjeta y los datos que contiene la banda magnética durante la transmisión de los mismos. Si una parte no autorizada obtiene el número de la tarjeta en modo alguno, se ha producido una violación de la confidencialidad.

La pérdida de la confidencialidad de la información puede adoptar muchas formas. Cuando alguien mira por encima de su hombro, mientras usted tiene información confidencial en la pantalla, cuando se publica información privada, cuando un laptop con información sensible sobre una empresa es robado, cuando se divulga información confidencial a través del teléfono, etc. Todos estos casos pueden constituir una violación de la confidencialidad.

Integridad

Para la Seguridad de la Información, la integridad es la propiedad que busca mantener los datos libres de modificaciones no autorizadas. (No es igual a integridad referencial en bases de datos.) La violación de integridad se presenta cuando un empleado, programa o proceso (por accidente o con mala intención) modifica o borra los datos importantes que son parte de la información, así mismo hace que su contenido permanezca inalterado a menos que sea modificado por personal autorizado, y esta modificación sea registrada, asegurando su precisión y confiabilidad. La integridad de un mensaje se obtiene adjuntándole otro conjunto de datos de comprobación de la integridad: la firma digital Es uno de los pilares fundamentales de la seguridad de la información

Disponibilidad

La Disponibilidad es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.

En el caso de los sistemas informáticos utilizados para almacenar y procesar la información, los controles de seguridad utilizados para protegerlo, y los canales de comunicación protegidos que se utilizan para acceder a ella deben estar

funcionando correctamente. La Alta disponibilidad sistemas objetivo debe seguir estando disponible en todo momento, evitando interrupciones del servicio debido a cortes de energía, fallos de hardware, y actualizaciones del sistema.

Garantizar la disponibilidad implica también la prevención de ataque Denegación de servicio.

La disponibilidad además de ser importante en el proceso de seguridad de la información, es además variada en el sentido de que existen varios mecanismos para cumplir con los niveles de servicio que se requiera, tales mecanismos se implementan en infraestructura tecnológica, servidores de correo electrónico, de bases de datos, de web etc., mediante el uso de clusters o arreglos de discos, equipos en alta disponibilidad a nivel de red, servidores espejo, replicación de datos, redes de almacenamiento (SAN), enlaces redundantes, etc. La gama de posibilidades dependerá de lo que queremos proteger y el nivel de servicio que se quiera proporcionar.

No repudio

Evitar el repudio de información constituye la garantía de que ninguna de las partes involucradas pueda negar en el futuro una operación realizada.

Autenticación

La autenticación consiste en la confirmación de la identidad de un usuario; es decir, la garantía para cada una de las partes de que su interlocutor es realmente quien dice ser. Un control de acceso permite (por ejemplo gracias a una contraseña codificada) garantizar el acceso a recursos únicamente a las personas autorizadas.

Necesidad de un enfoque global

Frecuentemente, la seguridad de los sistemas de información es objeto de

metáforas. A menudo, se la compara con una cadena, afirmándose que el nivel de seguridad de un sistema es efectivo únicamente si el nivel de seguridad del eslabón más débil también lo es. De la misma forma, una puerta blindada no sirve para proteger un edificio si se dejan las ventanas completamente abiertas.

Lo que se trata de demostrar es que se debe afrontar el tema de la seguridad a nivel global y que debe constar de los siguientes elementos:

- **Concienciar a los usuarios acerca de los problemas de seguridad.**
- **Seguridad lógica**, es decir, la seguridad a nivel de los datos, en especial los datos de la empresa, las aplicaciones e incluso los sistemas operativos de las compañías.
- **Seguridad en las telecomunicaciones:** tecnologías de red, servidores de compañías, redes de acceso, etc.
- **Seguridad física**, o *la seguridad de infraestructuras materiales*: asegurar las habitaciones, los lugares abiertos al público, las áreas comunes de la compañía, las estaciones de trabajo de los empleados, etc. [13]

2.5.2. Estrategia de Seguridad de la Información

Para establecer una estrategia adecuada es conveniente pensar una política de protección en los distintos niveles que esta debe.

En cada caso considerado, el plan de seguridad debe incluir una estrategia Proactiva y Reactiva.[14]

La Estrategia Proactiva (proteger y proceder) o de previsión de ataques es un

[13] http://es.kioskea.net/contents/secu/secuintro.php3

[14] BENSON, Christopher. Estrategias de Seguridad. Inobis Consulting Pty Ltd. Microsoft © Solutions. http://www.microsoft.com/latam/technet/articulos/200011

conjunto de pasos que ayuda a reducir al mínimo la cantidad de puntos vulnerables existentes en las directivas de seguridad y a desarrollar planes de contingencia. La determinación del daño que un ataque va a provocar en un sistema y las debilidades y puntos vulnerables explotados durante este ataque ayudará a desarrollar esta estrategia.

La Estrategia Reactiva (perseguir y procesar) o estrategia posterior al ataque ayuda al personal de seguridad a evaluar el daño que ha causado el ataque, a repararlo o a implementar el plan de contingencia desarrollado en la estrategia Proactiva, a documentar y aprender de la experiencia, y a conseguir que las funciones comerciales se normalicen lo antes posible.

Con respecto a la postura que puede adoptarse ante los recursos compartidos:

- Lo que no se permite expresamente está prohibido: significa que la organización proporciona una serie de servicios bien determinados y documentados, y cualquier otra cosa está prohibida.
- Lo que no se prohíbe expresamente está permitido: significa que, a menos que se indique expresamente que cierto servicio no está disponible, todos los demás sí lo estarán.

Estas posturas constituyen la base de todas las demás políticas de seguridad y regulan los procedimientos puestos en marcha para implementarlas. Se dirigen a describir qué acciones se toleran y cuáles no.

Actualmente, y "gracias" a las, cada día más repetitivas y eficaces, acciones que atentan contra los sistemas informáticos los expertos se inclinan por recomendar la primera política mencionada.

1. Implementación
2. Auditoría y Control
3. Plan de Contingencia
4. Equipos de Respuesta a Incidentes
5. Backups
6. Pruebas

Implementación de una Política de Seguridad de la información

La implementación de medidas de seguridad, es un proceso Técnico-Administrativo. Como este proceso debe abarcar toda la organización, sin exclusión alguna, ha de estar fuertemente apoyado por el sector gerencial, ya que sin ese apoyo, las medidas que se tomen no tendrán la fuerza necesaria.

Se deberá tener en cuenta que la implementación de Políticas de Seguridad, trae aparejados varios tipos de problemas que afectan el funcionamiento de la organización. La implementación de un sistema de seguridad conlleva a incrementar la complejidad en la operatoria de la organización, tanto técnica como administrativamente.

Por esto, será necesario sopesar cuidadosamente la ganancia en seguridad respecto de los costos administrativos y técnicos que se generen.

Es fundamental no dejar de lado la notificación a todos los involucrados en las nuevas disposiciones y, darlas a conocer al resto de la organización con el fin de otorgar visibilidad a los actos de la administración.

Una PSI deberá abarcar:

- Alcance de la política, incluyendo sistemas y personal sobre el cual se aplica.
- Objetivos de la política y descripción clara de los elementos involucrados en su definición.
- Responsabilidad de cada uno de los servicios, recurso y responsables en todos los niveles de la organización.
- Responsabilidades de los usuarios con respecto a la información que generan y a la que tienen acceso.
- Requerimientos mínimos para la configuración de la seguridad de los sistemas al alcance de la política.
- Definición de violaciones y las consecuencias del no cumplimiento de la política.

- Por otra parte, la política debe especificar la autoridad que debe hacer que las cosas ocurran, el rango de los correctivos y sus actuaciones que permitan dar indicaciones sobre la clase de sanciones que se puedan imponer. Pero, no debe especificar con exactitud qué pasara o cuándo algo sucederá; ya que no es una sentencia obligatoria de la ley.
- Explicaciones comprensibles (libre de tecnicismos y términos legales pero sin sacrificar su precisión) sobre el porqué de las decisiones tomadas.
- Finalmente, como documento dinámico de la organización, deben seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes: crecimiento de la planta de personal, cambio en la infraestructura computacional, alta y rotación de personal, desarrollo de nuevos servicios, cambio o diversificación de negocios, etc. [15]

Para implantar la política de seguridad se comienza realizando una evaluación del factor humano, el medio en donde se desempeña, los mecanismos con los cuales se cuenta para llevar a cabo la tarea encomendada, las amenazas posibles y sus posibles consecuencias.

Luego de evaluar estos elementos y establecida la base del análisis, se originan un programa de seguridad, el plan de acción y las normas y procedimientos a llevar a cabo.

Para que todo lo anterior llegue a buen fin debe realizarse un control periódico de estas políticas, que asegure el fiel cumplimiento de todos los procedimientos enumerados. Para asegurar un marco efectivo se realiza una auditoría a los archivos Logs de estos controles.

Con el objeto de confirmar que todo lo creado funciona en un marco real, se realiza una simulación de eventos y acontecimientos que atenten contra la seguridad del sistema. Esta simulación y los casos reales registrados generan

[15] "Encuesta de Seguridad Informática 2001". Marzo de 2001. Ernst & Young. http://www.ey.com

una realimentación y revisión que permiten adecuar las políticas generadas en primera instancia.

Por último el Plan de Contingencia es el encargado de suministrar el respaldo necesario en caso en que la política falle.

Es importante destacar que la Seguridad debe ser considerada desde la fase de diseño de un sistema. Si la seguridad es contemplada luego de la implementación del mismo, el personal se enfrentará con problemas técnicos, humanos y administrativos muchos mayores que implicaran mayores costos para lograr, en la mayoría de los casos, un menor grado de seguridad.

Queda claro que este proceso es dinámico y continuo, sobre el que hay que adecuarse continuamente a fin de subsanar inmediatamente cualquier debilidad descubierta, con el fin de que estas políticas no caigan en desuso.[16]

Auditoría y Control

Se considera que la Auditoría son los "ojos y oídos" de la dirección, que generalmente no puede, no sabe o no debe realizar las verificaciones y evaluaciones.

La Auditoría consiste en contar con los mecanismos para poder determinar qué es lo que sucede en el sistema, qué es lo que hace cada uno y cuando lo hace.

En cuanto al objetivo del Control es contrastar el resultado final obtenido contra el deseado a fin de incorporar las correcciones necesarias para alcanzarlo, o bien verificar la efectividad de lo obtenido.

Plan de Contingencia

Pese a todas las medidas de seguridad puede (va a) ocurrir un desastre. De

[16] ARDITA, Julio César. Director de Cybsec S.A. Security System y ex-Hacker. Entrevista personal realizada el día 15 de enero de 2001 en instalaciones de Cybsec S.A. http://www.cybsec.com

hecho los expertos en seguridad afirman "sutilmente" que hay que definir un plan de recuperación de desastres "para cuando falle el sistema", no "por si falla el sistema.

Por tanto, es necesario que el Plan de Contingencias que incluya un plan de recuperación de desastres, el cual tendrá como objetivo, restaurar el servicio de cómputo en forma rápida, eficiente y con el menor costo y pérdidas posibles.
Si bien es cierto que se pueden presentar diferentes niveles de daños, también se hace necesario presuponer que el daño ha sido total, con la finalidad de tener un Plan de Contingencias lo más completo y global posible.

Un Plan de Contingencia de Seguridad de la Información consiste los pasos que se deben seguir, luego de un desastre, para recuperar, aunque sea en parte, la capacidad funcional del sistema aunque, y por lo general, constan de reemplazos de dichos sistemas.

Se entiende por Recuperación, "tanto la capacidad de seguir trabajando en un plazo mínimo después de que se haya producido el problema, como la posibilidad de volver a la situación anterior al mismo, habiendo reemplazado o recuperado el máximo posible de los recursos e información[17]

Se dice que el Plan de Contingencias es el encargado de sostener el modelo de Seguridad Informática planteado y de levantarlo cuando se vea afectado.

La recuperación de la información se basa en el uso de una política de copias de seguridad (Backup) adecuada.

[17] POYATO, Chelo. COLL, Francisco. MORENO, David. Recomendaciones de Seguridad. Definición de una Política de Seguridad.
http://www.rediris.es/cert/doc/docu_rediris/recomendaciones/html/recomendaciones.html

Equipos de Respuesta a Incidentes

Es aconsejable formar un equipo de respuesta a incidentes. Este equipo debe estar implicado en los trabajos proactivos del profesional de la seguridad. Entre éstos se incluyen:

- El desarrollo de instrucciones para controlar incidentes.
- Creación del sector o determinación del responsable: usualmente la designación del Administrador de seguridad.
- La identificación de las herramientas de software para responder a incidentes y eventos.
- La investigación y desarrollo de otras herramientas de Seguridad Informática.
- La realización de actividades formativas y de motivación.
- La realización de investigaciones acerca de virus.
- La ejecución de estudios relativos a ataques al sistema.

Estos trabajos proporcionarán los conocimientos que la organización puede utilizar y la información que hay que distribuir antes y durante los incidentes.

Una vez que el Administrador de seguridad y el equipo de respuesta a incidentes han realizado estas funciones proactivas, el Administrador debe delegar la responsabilidad del control de incidentes al equipo de respuesta.

Esto no significa que el Administrador no deba seguir implicado o formar parte del equipo, sino que no tenga que estar siempre disponible, necesariamente, y que el equipo debe ser capaz de controlar los incidentes por sí mismo.

El equipo será el responsable de responder a incidentes como virus, gusanos o cualquier otro código dañino, invasión, engaños, y ataques del personal interno. El equipo también debe participar en el análisis de cualquier evento inusual que pueda estar implicado en la seguridad de los equipos o de la red.

Backups / Copias de Seguridad

El **Backup** de archivos permite tener disponible e íntegra la información para cuando sucedan los accidentes. Sin un backup, simplemente, es imposible volver la información al estado anterior al desastre.

Como siempre, será necesario realizar un análisis Costo/Beneficio para determinar qué información será almacenada, los espacios de almacenamiento destinados a tal fin, la forma de realización, las estaciones de trabajo que cubrirá el backup, etc.

Para una correcta realización y seguridad de backups se deberán tener en cuenta estos puntos:

1. Se debe de contar con un procedimiento de respaldo de los sistemas operativos y de la información de los usuarios, para poder reinstalar fácilmente en caso de sufrir un accidente.
2. Se debe determinar el medio y las herramientas correctas para realizar las copias, basándose en análisis de espacios, tiempos de lectura/escritura, tipo de backup a realizar, etc.
3. El almacenamiento de los Backups debe realizarse en locales diferentes de donde reside la información primaria. De este modo se evita la pérdida si el desastre alcanza todo el edificio o local.
4. Se debe verificar, periódicamente, la integridad de los respaldos que se están almacenando. No hay que esperar hasta el momento en que se necesitan para darse cuenta de que están incompletos, dañados, mal almacenados, etc.
5. Se debe de contar con un procedimiento para garantizar la integridad física de los respaldos, en previsión de robo o destrucción.
6. Se debe contar con una política para garantizar la privacidad de la información que se respalda en medios de almacenamiento secundarios. Por ejemplo, la información se debe encriptar antes de respaldarse.
7. Se debe de contar con un procedimiento para borrar físicamente la información de los medios de almacenamiento, antes de desecharlos.

Se debe asegurar reproducir toda la información necesaria para la posterior recuperación sin pasos secundarios.

Pruebas y Evaluación de Resultados

El último elemento de las estrategias de seguridad, las pruebas y el estudio de sus resultados, se lleva a cabo después de que se han puesto en marcha las estrategias reactiva y proactiva. La realización de ataques simulados (Ethical Hacking) en sistemas de pruebas o en laboratorios permiten evaluar los lugares en los que hay puntos vulnerables y ajustar las directivas y los controles de seguridad en consecuencia.

Estas pruebas no se deben llevar a cabo en los sistemas de producción real, ya que el resultado puede ser desastroso. La carencia de laboratorios y equipos de pruebas a causa de restricciones presupuestarias puede imposibilitar la realización de ataques simulados.

Para asegurar los fondos necesarios para las pruebas, es importante que los directivos sean conscientes de los riesgos y consecuencias de los ataques, así como de las medidas de seguridad que se pueden adoptar para proteger al sistema, incluidos los procedimientos de las pruebas. Si es posible, se deben probar físicamente y documentar todos los casos de ataque para determinar las mejores directivas y controles de seguridad posibles que se van a implementar.

Determinados ataques, por ejemplo desastres naturales como inundaciones y rayos, no se pueden probar, aunque una simulación servirá de gran ayuda. Por ejemplo, se puede simular un incendio en la sala de servidores en el que todos los servidores hayan resultado dañados y hayan quedado inutilizables. Este caso puede ser útil para probar la respuesta de los Administradores y del personal de seguridad, y para determinar el tiempo que se tardará en volver a poner la organización en funcionamiento.

La realización de pruebas y de ajustes en las directivas y controles de seguridad en función de los resultados de las pruebas es un proceso iterativo de aprendizaje. Nunca termina, ya que debe evaluarse y revisarse de forma periódica para poder implementar mejoras.

2.5.3. Las amenazas a la seguridad de información.

Una vez que la programación y el funcionamiento de un dispositivo de almacenamiento (o transmisión) de la información se consideran seguras, todavía deben ser tenidos en cuenta las circunstancias "no informáticas" que pueden afectar a los datos, las cuales son a menudo imprevisibles o inevitables, de modo que la única protección posible es la redundancia (en el caso de los datos) y la descentralización -por ejemplo mediante estructura de redes- (en el caso de las comunicaciones).

Estos fenómenos pueden ser causados por:

- El usuario: causa del mayor problema ligado a la seguridad de un sistema informático (porque no le importa, no se da cuenta o a propósito).
- Programas maliciosos: programas destinados a perjudicar o a hacer un uso ilícito de los recursos del sistema. Es instalado (por inatención o maldad) en el ordenador abriendo una puerta a intrusos o bien modificando los datos. Estos programas pueden ser un virus informático, un gusano informático, un troyano, una bomba lógica o un programa espía o Spyware.
- Un intruso: persona que consigue acceder a los datos o programas de los cuales no tiene acceso permitido (cracker, defacer, script kiddie o *Script boy*, viruxer, etc.).
- Un siniestro (robo, incendio, inundación): una mala manipulación o una mal intención derivan a la pérdida del material o de los archivos.
- El personal interno de Sistemas. Las pujas de poder que llevan a disociaciones entre los sectores y soluciones incompatibles para la seguridad informática.

Tipos de amenaza

El hecho de conectar una red a un entorno externo nos da la posibilidad de que algún atacante pueda entrar en ella, con esto, se puede hacer robo de información o alterar el funcionamiento de la red. Sin embargo el hecho de que la red no sea conectada a un entorno externo no nos garantiza la seguridad de la misma. De acuerdo con el Computer Secutiry Institute (CSI) de San Francisco aproximadamente entre 60 y 80 por ciento de los incidentes de red son causados desde adentro de la misma. Basado en esto podemos decir que existen 2 tipos de amenazas:

- **Amenazas internas:** Generalmente estas amenazas pueden ser más serias que las externas por varias razones como son:

  - Los usuarios conocen la red y saben cómo es su funcionamiento.

  - Tienen algún nivel de acceso a la red por las mismas necesidades de su trabajo.

  - Los IPS y Firewalls son mecanismos no efectivos en amenazas internas.

- **Amenazas externas**: Son aquellas amenazas que se originan de afuera de la red. Al no tener información certera de la red, un atacante tiene que realizar ciertos pasos para poder conocer qué es lo que hay en ella y buscar la manera de atacarla. La ventaja que se tiene en este caso es que el administrador de la red puede prevenir una buena parte de los ataques externos. [18]

[18] http://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica

2.5.4. COMBATIR AMENAZAS.

GFI Report Center

Herramienta que identifica vulnerabilidades en los sistemas operativos, ayudándonos de esta forma en el proceso de identificación de vulnerabilidades.

Utilizamos esta herramienta para:

- Búsqueda de vulnerabilidades en su red (Windows y Linux)
- Directorios compartidos, puertos abiertos, cuentas no usadas.
- Revisión de actualizaciones aplicadas en los sistemas operativos.
- Detección de dispositivos USB

GFI ReportCenter es un marco centralizado de generación de informes que le ayuda a generar varios informes utilizando la información recogida por diferentes GFI ReportPacks. Un Report Pack es un conjunto de informes especializados, creados y publicados para cada uno de nuestros productos; por ejemplo, GFI EventsManager ReportPack. Los ReportPack se integran en el marco GFI ReportCenter; le permiten generar, analizar, exportar e imprimir la información generada por cualquier producto GFI.

Las características clave del marco GFI ReportCenter incluyen:

- **Informes Centralizados:**

  Un marco de generación de informes centralizado que le proporciona la capacidad de generar y personalizar informes gráficos y tabulados para una amplia familia de Productos GFI.

- **Informes Predefinidos y A Medida:**

  Cada ReportPack incluye un conjunto predefinido de informes gráficos y tabulados y además le permite crear informes a medida.

- **Programación de Informes:**

  Con GFI ReportCenter puede programar los informes para que sean generados mediante una programación predefinida así como a intervalos especificados.

- **Impresión o Exportación de Informes en Varios Formatos:**

  Por defecto, GFI ReportCenter le permite exportar los informes en varios formatos. Los formatos soportados incluyen HTML, PDF, XLS, DOC y RTF. También hay disponibles versiones imprimibles de los informes.

- **Reparto de Informes mediante Correo Electrónico:**

  GFI ReportCenter le permite repartir automáticamente por correo los informes generados.

- **Configuración Asistida:**

  Se proporcionan asistentes para ayudarlo en la configuración, programación y personalización de informes.

- **Marque sus Informes Favoritos:**

  GFI ReportCenter le permite crear favoritos de los informes que utilice más frecuentemente, tanto predefinidos como a medida.

2.5.5. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Con sus siglas SGSI el Sistema de Gestión de Seguridad de la información ayuda a establecer políticas, procedimientos y controles en relación a los objetivos del negocio de la organización**,** con el objeto de mantener siempre el riesgo por debajo del nivel asumible de la propia organización.

Un SGSI es, tal como su nombre lo indica, un elemento para administración relacionado con la seguridad de la información, aspecto fundamental de cualquier empresa. Un SGSI implica crear un plan de diseño, implementación, y mantenimiento de una serie de procesos que permitan gestionar de manera eficiente la información, para asegurar la integridad, confidencialidad y disponibilidad de la información.

Toda organización tiene objetivos, por lo general relacionados con el mercado y los negocios, y requiere que desde los procesos de operaciones hasta las políticas de uso de recursos, sean definidos a un nivel general, de manera confiable. Si bien gran parte de la información se vincula con computadoras y redes, hay otra parte que no se representa en forma de bits, sino por ejemplo en papeles, en la memoria de las personas, en el conocimiento y experiencia de la organización misma, en la madurez de sus procesos, etc. En ambos casos, la información debe ser protegida de manera diferente, y aquí entra en juego un SGSI.

Por lo general es posible disminuir el impacto de los riesgos potenciales sin necesidad de grandes cambios, pero a la vez es necesaria la planificación e implantación de ciertos controles basados en un cuidadoso análisis de riesgo.

Un SGSI ayuda a mantener este riesgo por debajo del nivel aceptable que se haya determinado a nivel directivo.

Muchas organizaciones creen que implementar un SGSI es demasiado esfuerzo, y está solo destinado a grandes corporaciones, lo que a veces termina derivando en un manejo caótico o muy minimalista de la administración

de la seguridad. Sin embargo es posible en algunos casos aplicar unos pocos principios, en lugar de un SGSI completo, para conseguir mejoras significativas.

Para esto será necesario olvidar las formalidades del cumplimiento de una norma, pero sin dejar de seguir sus lineamientos principales.

Desde el punto de vista de la alta gerencia, un SGSI permite obtener una visión global del estado de los sistemas de información sin caer en detalles técnicos, además de poder observar las medidas de seguridad aplicadas y los resultados obtenidos, para poder con todos estos elementos tomar mejores decisiones estratégicas. Otro punto importante es que un SGSI debe estar documentado y ser conocido a distintos niveles por todo el personal, y estar incluido en un proceso global que permita la mejora continua.

Un SGSI debe ser considerado a la hora de administrar la seguridad en una organización, en especial cuando la estructura cuenta con un alto nivel de complejidad, para conseguir así una mayor eficiencia y garantía en la protección de sus activos de información.[19]

¿Cómo Implantar un SGSI?

SGS puede asesorar y guiarle en cada uno de los pasos para implantar un SGSI.

El primer paso es definir el ámbito de aplicación de la política del SGSI. Este paso es crítico para identificar los peligros potenciales a los que se enfrenta y decidir una metodología sistemática para evaluar esos riesgos. Una vez realizado, Un SGSI apropiado incluye los pasos de implantación, puesta en funcionamiento, revisión, mantenimiento y mejora del sistema descritos en el estándar.

[19] http://blogs.eset-la.com/laboratorio/2010/09/10/la-importancia-de-un-sgsi/

2.5.6. NORMA ISO 27001

El estándar para la seguridad de la información ISO/IEC 27001 fue aprobado y publicado como estándar internacional en octubre de 2005.

Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI) según el conocido “Ciclo de Deming”: PDCA - acrónimo de **P**lan, **D**o, **C**heck, **A**ct (Planificar, Hacer, Verificar, Actuar). Es consistente con las mejores prácticas descritas en ISO/IEC 17799 (actual ISO/IEC 27002) y tiene su origen en la norma BS 7799-2:2002, desarrollada por la entidad de normalización británica, la (BSI).

Implantación

La implantación de ISO/IEC 27001 en una organización es un proyecto que suele tener una duración entre 6 y 12 meses, dependiendo del grado de madurez en seguridad de la información y el alcance, entendiendo por alcance el ámbito de la organización que va a estar sometido al Sistema de Gestión de la Seguridad de la Información (en adelante SGSI) elegido. En general, es recomendable la ayuda de consultores externos.

Aquellas organizaciones que hayan adecuado previamente de forma rigurosa sus sistemas de información y sus procesos de trabajo a las exigencias de las normativas legales de protección de datos o que hayan realizado un acercamiento progresivo a la seguridad de la información mediante la aplicación de las buenas prácticas de ISO/IEC 27002, partirán de una posición más ventajosa a la hora de implantar ISO/IEC 27001.

El equipo de proyecto de implantación debe estar formado por representantes de todas las áreas de la organización que se vean afectadas por el SGSI, liderado por la dirección y asesorado por consultores externos especializados en seguridad informática, derecho de las nuevas tecnologías, protección de datos y sistemas de gestión de seguridad de la información (que hayan realizado un curso de implantador de SGSI).

Los ocho capítulos de ISO 27001 son:

1. Alcance
   1.1. General
   1.2. Aplicación
2. Referencias normativas
3. Términos y definiciones
4. Sistema de gestión de seguridad de la información
   4.1. Requerimientos generales
   4.2. Establecer y manejar el SGSI
   4.3. Requerimientos de documentación
5. Responsabilidad de la gerencia
   5.1. Compromiso de la gerencia
   5.2. Gestión de recursos
6. Auditorías internas SGSI
7. Revisión Gerencial del SGSI
   7.1. General
   7.2. Insumo de la revisión
   7.3. Resultado de la revisión
8. Mejoramiento del SGSI
   8.1. Mejoramiento contínuo
   8.2. Acción correctiva
   8.3. Acción preventiva

2.5.7. CASOS DE ÉXITO DE IMPLANTACIÓN DE NORMA ISO 27001

1.- CONSOLTIC

Figura # 9. Logo de CONSOLTIC.

Fuente: http://www.consoltic.com/#axzz17faQMCAR

Origen: Madrid-España

Fecha de Implementación: 20-03-2008

CONSOLTIC

Somos un **equipo de emprendedores** y profesionales especializados en el sector de las Tecnologías de la Información y la Comunicación. La empresa fue fundada en el año 2003 y se dedica desde entonces a proporcionar servicios integrales de consultoría y soluciones en TIC a la medida de las necesidades de la Empresa de cara al futuro.

CONSOLTIC ha obtenido la certificación de AENOR ISO 27001 (SGSI). Esta iniciativa promovida por ETICOM, dentro de su programa Pymética Seguridad proyecta situar a esta como una de las primeras comunidad en cuanto a empresas certificadas en SGSI.

Tras conseguir esta certificación, CONSOLTIC empezó a sentir mejoras en los siguientes aspectos:

- Garantía de un elevado nivel de confidencialidad gracias a la reducción de los riesgos asociados.
- Garantía de un elevado nivel de disponibilidad gracias a la implementación de un centro de datos de elevada disponibilidad y redundancia y de un centro de disaster recovery que se podrá utilizar en caso de catástrofe;
- Mayor calidad de los servicios ofrecidos a los clientes como consecuencia de una mayor uniformidad y control de los procesos organizativos y de especificación, desarrollo y evaluación del software.
- Desarrollo y motivación de los recursos humanos mediante la responsabilización, sensibilización y formación continua en seguridad;

2.- PiN Producción Informática.

Figura # 8. Logo PiN Producción Informática.

Fuente: http://www.pinsl.es

Origen: España

Fecha de Implementación: 15-01-2010

CERTIFICACIÓN DE UN SISTEMA INTEGRADO EN ISO27001

Dentro de los servicios de TIC que presta PINSL, su capital humano, infraestructura y sistemas son importantes activos. Definir, realizar, mantener y mejorar la seguridad de la información, son esenciales para asegurar la mejora continua de la calidad del servicio y su cumplimiento legal.

Dentro de los proyectos técnicos de TIC, la componente económica es la que prima. Dentro de un Sistema de Gestión, la componente organizativa y de sincronización de recursos humanos es la que prima. Un Sistema Integrado de Gestión (ISO 27001), nos lleva a adquirir un compromiso de vigilancia y mejora continua de la seguridad de nuestra información, haciendo más ágil y sencilla la implantación y explotación de cualquier sistema TIC a abordar.

Resultados - Beneficios (entidad y/o ciudadano)

Producción Informática de Navarra, S.L. ha podido conocer y valorar los riesgos a los que están sometidos sus activos de información y además los gestionarlos mediante una metodología definida, documentada y conocida por el personal de la empresa, clientes y proveedores, que se revisa, se mejora y audita por terceros. Contar con un sistema de gestión integrado de seguridad de la información permite ordenar las actividades de PINSL, dirigirlas hacia el objetivo marcado, reaccionar ante hechos que pueden ser previstos y

gestionados adecuadamente antes de que lleguen a ser un problema. Este método de trabajo es una manera eficaz de ahorrar costes y minimizar riesgos, obteniendo los siguientes beneficios:

- Reducción de costes.
- Optimización de recursos e inversiones en tecnología.
- Protección y recuperación del negocio
- Mejora de la competitividad
- Cumplimiento legal y reglamentario.
- Mantener y mejorar la imagen corporativa

Para mayor información del proceso de éxito de PINSL, puede visitar la página:

www.aslan.es/files/1149-21496-Archivo/certificacionnavarra.pdf

CAPÍTULO III

SITUACIÓN ACTUAL DE LA EMPRESA LST (Logística y Servicios Tecnológicos)

ANTECEDENTES

3.1.1. Quienes Somos

Figura#10. Logotipo de LST

Fuente: http://www.lstecuador.com

Sobre nosotros

Somos un grupo de profesionales expertos en diversas áreas de tecnología y gestión de proyectos, dispuestos a darles soluciones que permitan su mejoramiento empresarial, mediante soluciones integrales prácticas, versátiles y bajo software libre.

3.1.2. Misión

Brindar servicios y productos que mejoren la gestión de las empresas mediantes aplicaciones tecnológicas adecuadas.

3.1.3. Visión

Consolidarnos como una empresa de soluciones integrales tecnológicas.

3.1.4. Objetivos Estratégicos

1. Desarrollar soluciones empresariales basadas en tecnología de software libre
    1.1. Desarrollo de aplicaciones virtuales

    1.2. Desarrollo de aplicaciones websoft

2. Crecer la participación de mercado en el sector empresarial, público y privado

    2.1. Implementar campañas de marketing

    2.2. Generar convenios de cooperación empresarial

3. Consolidarnos como un centro de capacitación en software libre

    3.1. Elaborar contenidos y material para cursos GNU

3.2 EXPERIENCIA OBTENIDA

3.2.1. PRINCIPALES INCONVENIENTES

- Falta de conocimiento profundo sobre ciertos programas de software libre
- Desconfianza de ciertas empresas y usuarios en aplicaciones de software libre
- Desarrollo sin metodología estándar
- No se encuentra técnicos experimentados en el mercado local a precios accesibles

3.2.2. PRINCIPALES TRIUNFOS

- Desarrollo de páginas web en software libre para grandes empresas
- Capacitación a varias empresas públicas, privadas y principalmente entidades educativas
- Buen posicionamiento de nuestros servicios en la web

3.3. ANALISIS Y DESCRIPCIÓN DEL MODELO DE NEGOCIOS DE LST (Logística y Servicios Tecnológicos)

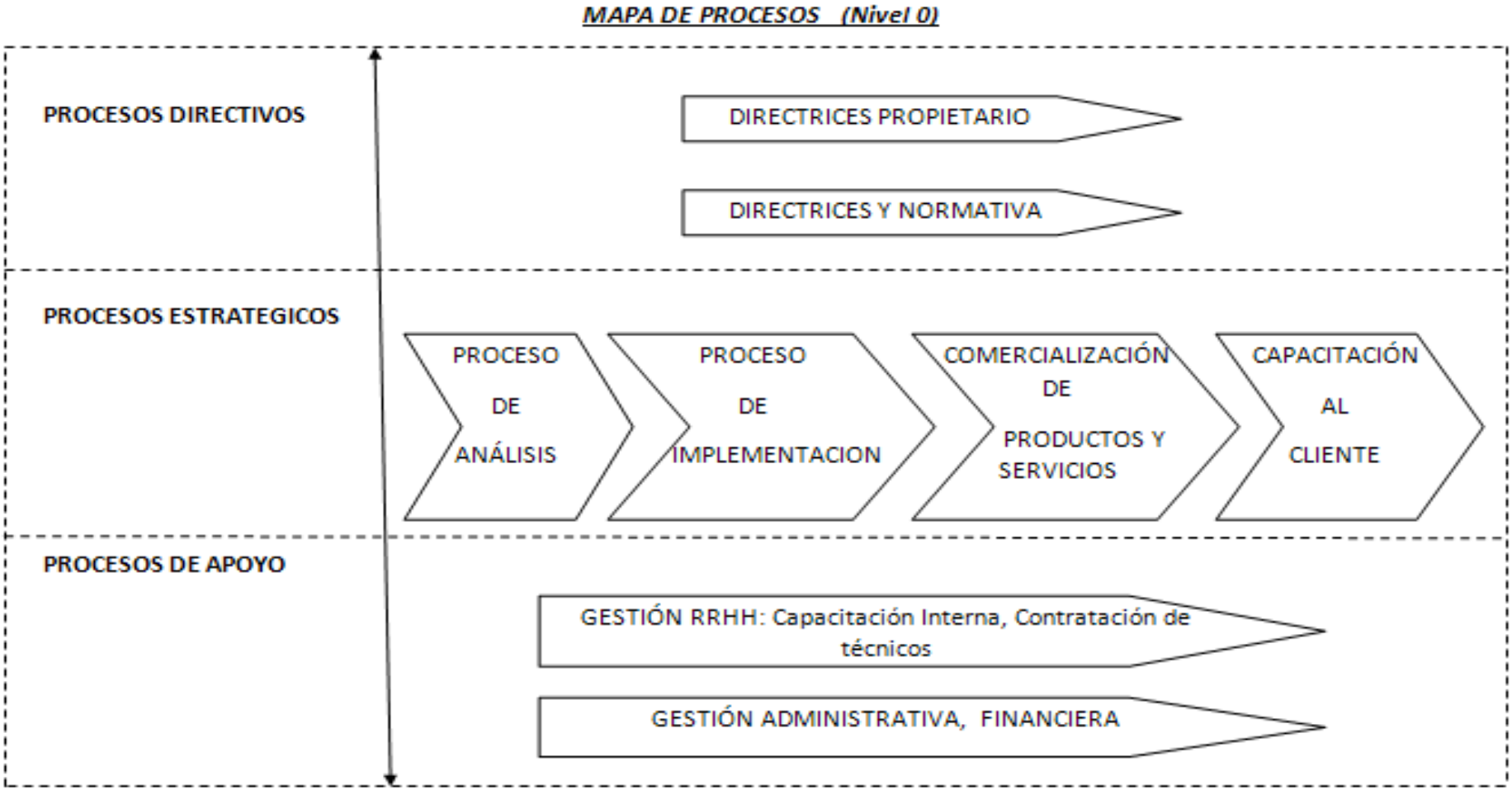


Figura #11. Mapa de procesos de LST Nivel 0

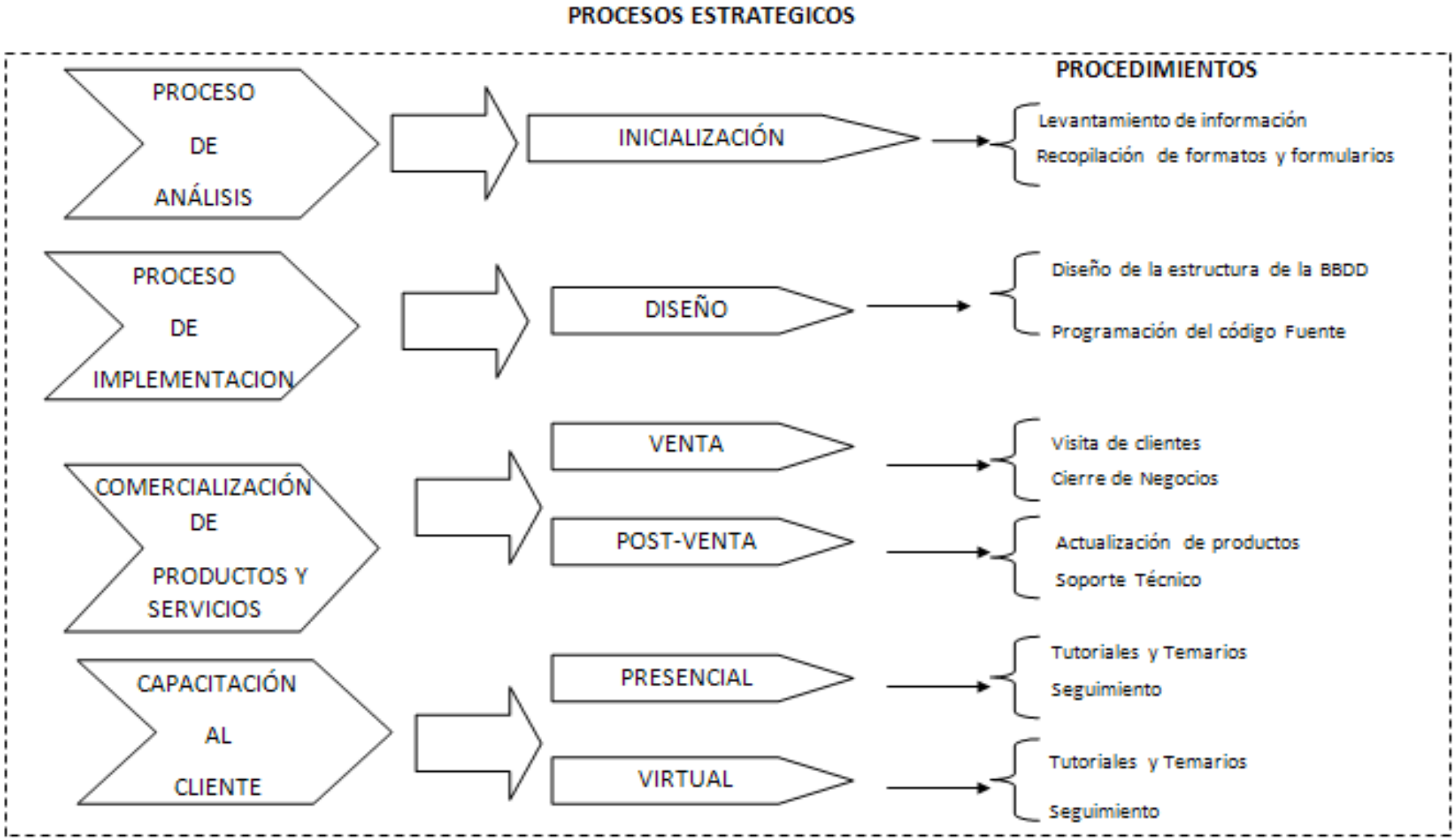


Figura #12.Procesos Estratégicos de LST

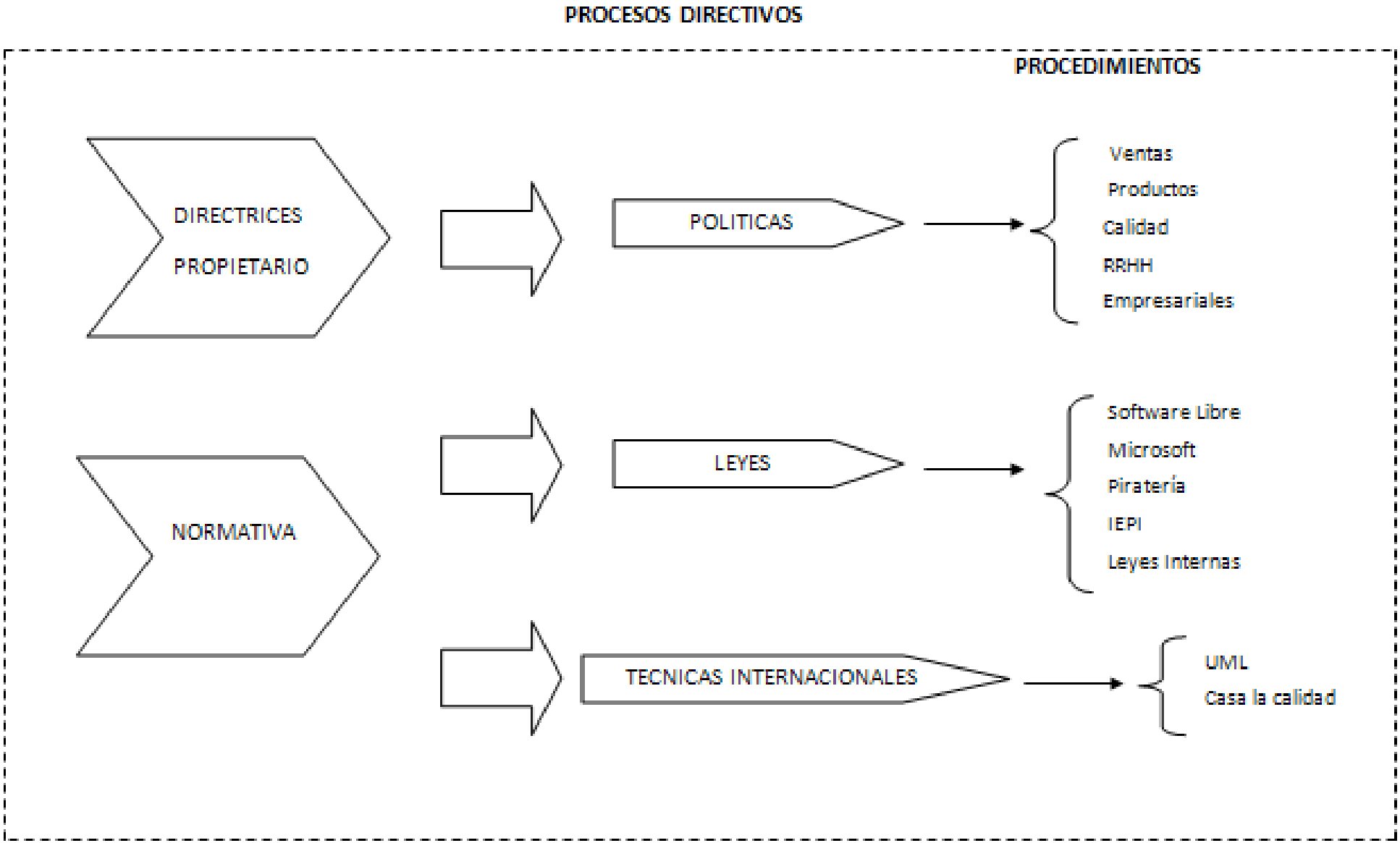


Figura #13. Sub procesos de los procesos Directivos de LST

SUB PROCESOS Y TAREAS EN LST

PROCESOS ESTRATÉGICOS

- **ANÁLISIS**
  - **INICIALIZACIÓN**
    - **Levantamiento de información**
      - Recopilación de datos
      - Recopilación de información
      - Identificar problemas iniciales
      - Oportunidades de mejora.
    - **Recopilación de formatos y formularios**
      - Investigación de tipos de formatos y formularios
      - Revisión de formatos y formularios
      - Elección de formatos y formularios
- **IMPLEMENTACIÓN**
  - **DISEÑO**
    - **Diseño de la estructura de la BBDD**
      - Familiarización con tablas, formularios, etc.
      - Introducción de datos
      - Búsqueda y reemplazo de datos
      - Ejecución de consultas.
    - **Programación del código Fuente**
      - Programación inicial
      - Limpieza de programación
      - Obtención de el programa ejecutable
- **COMERCIALIZACIÓN DE PRODUCTOS Y SERVICIOS**
  - **VENTA**
    - **Visita de clientes**
      - Búsqueda de clientes Potenciales
      - Fidelización de clientes
    - **Cierre de Negocios**
      - Ofertas
      - Promociones

- **POST-VENTA**
  - **Actualización de productos**
    - Corrección de algún error
    - Observación de en que se puede mejorar
    - Realización de cambios
  - **Soporte Técnico**
    - Mantenimiento preventivo y correctivo
    - Instalación de Programas de Actualización.
    - Análisis, diagnósticos y sugerencias para mejorar un equipo informático
    - Recuperación de datos
    - Instalación de componentes adicionales

- ***CAPACITACIÓN AL CLIENTE***
  - **PRESENCIAL**
    - **Tutoriales y Temarios**
      - Diseño de metodología
      - Elaboración de material
    - **Seguimiento**
      - Evaluación
      - Proceso de Seguimiento
  - **VIRTUAL**
    - **Tutoriales y Temarios**
      - Diseño de metodología
      - Elaboración de material
    - **Seguimiento**
      - Evaluación
      - Proceso de Seguimiento

CAPÍTULO IV

4. Propuesta de un modelo de gestión para la Empresa: LST (Logística y Servicios Tecnológicos)

4.1. Modelo de Gestión de la Calidad, En base a la Norma ISO 9001

Manual de Calidad

Certificación ISO 9001:2008

Para:

0. Antecedentes

0.1 Información de la Organización

Somos un grupo de profesionales expertos en diversas áreas de tecnología y gestión de proyectos, dispuestos a darles soluciones que permitan su mejoramiento empresarial, mediante soluciones integrales prácticas, versátiles y bajo software libre

La organización tiene las siguientes funciones:

- Desarrollo de Páginas y software basado en Web
- Soluciones de Software a la medida
- Soporte técnico informático empresarial
- Capacitación Profesional Básica, Intermedia y Superior
- Soluciones Tecnológicas para la educación
- Soluciones tecnológicas para la salud
- Proyectos sociales
- Capacitación profesional
- Soluciones de video comunicación
- Soluciones de telecomunicación LAN, Wirless, WISP, y soporte técnico
- Soluciones medicas, judiciales, educativas y de seguridad ciudadana
- Diseño, Desarrollo y ejecución de Proyectos
- Soluciones de Planeación Estratégica
- Posicionamiento Web, para empresas con o sin página Web
- Soluciones de Comercio Electrónico
- Publicidad Electrónica
- Sistemas de Calidad ISO

0.2 Misión

Brindar servicios y productos que mejoren la gestión de las empresas mediantes aplicaciones tecnológicas adecuadas

0.3 Visión

Consolidarnos como una empresa de soluciones integrales tecnológicas

1. Objetivo y Alcance del Sistema de Gestión de Calidad

1.1 Objetivo.

El SGC en LST logística y Servicios Tecnológicos tiene por objetivo consolidarse en el desarrollo de soluciones empresariales basadas en tecnología de software libre

1.2 Alcance

El Sistema de Gestión de Calidad de LST se aplicara a todos los procesos de la organización

2. Referencias Normativas y Exclusiones

Referencia Normativa:

Sistema de Gestión de Calidad ISO 9001:2008.

El sistema de gestión de calidad de Logística y Servicios Tecnológicos, ISO 9001:2008 excluye a los siguientes requisitos establecidos en la Norma:

- 7.5.3 Propiedad del cliente, debido a que LST no recibe productos que deba preservar.

3. Definiciones

SGC.- Un **sistema de gestión de la calidad** es el conjunto de normas interrelacionadas de una organización por los cuales se administra de forma ordenada la calidad de la misma

Beneficiario.- Aquel que de forma no accidental hacen uso de los Productos Sustantivos de LST

.

Clientes.- usuarios de los procesos internos y externos.

Manual.- Se refiere al Manual del SGC.

Norma.- Norma IS0 9001:2008.

Objetivos Estratégicos.- Son objetivos que responden a las acciones que deben realizarse para dar cumplimiento a la Misión y Visión de toda la Organización, se consiguen en un largo plazo.

Objetivos Tácticos.- Son objetivos que se basan en la Misión, la Visión y en los Objetivos Estratégicos; se definen por unidad operacional de la Organización para conseguirlo a mediano plazo (“un año”).

Objetivos Operacionales.- Son objetivo que definen acciones particulares a ser llevados a cabo para lograr el cumplimiento de los objetivos tácticos, cada área y/o departamento los establece con la finalidad de lograrlo en el día a día.

Usuario.- Aquel que hace uso de la información de LST.

4. Descripción del Sistema de Gestión de Calidad

La conformación del SGC de LST surge del procedimiento metodológico descrito a continuación.

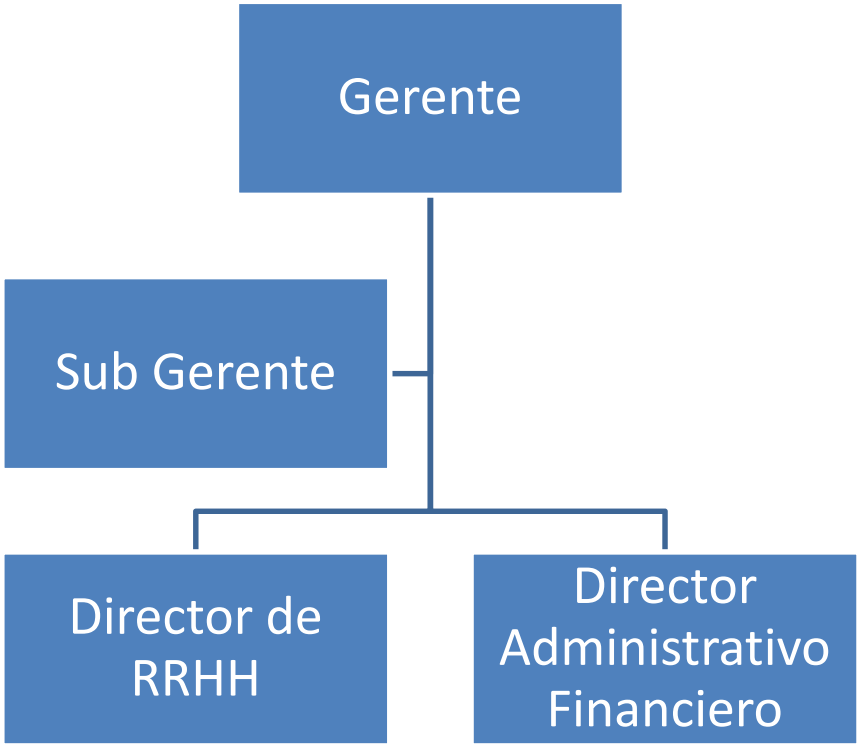
Debido al interés de una persona de proponer un modelo de gestión en base a la norma ISO 9001 partiendo de la lógica que para ofrecer Productos y

servicios a los Clientes, Beneficiarios y Usuarios, es necesario implementar un SGC, a través de la definición de procesos.

Esta propuesta fue organizada y analizada por el grupo de dirigentes con el que cuenta LST, y se llega a la conclusión de que sea propuesto, con el fin de ayudar a que LST funcione de una mejor manera, además que brinde confianza y seguridad a todos sus clientes.

Elementos que un SGC engloba:

1. Estructura organizacional de la Alta Dirección



Figura# 14. Estructura organizacional de la Alta Dirección

2. Estructura de responsabilidades

CARGO	*RESPONSABILIDADES*	*AUTORIDAD*
Gerente	Tener claro su propio trabajo Asignar tareas Asignar tareas ayudar a desarrollar a sus subordinados Evaluar la efectividad Hacerse responsables de su propia tarea y de la de los demás.	Autorizar los recursos necesarios Definir acciones Correctivas Definir acciones Preventivas Establecer mecanismos de comunicación Interna Autorizar documentos y registros necesarios
Subgerente	Vigilar que se cumplan reglamentos Participar en contratación de empleados Participar en negocios de contratos Programar la realización de proyectos Atender y dar seguimiento a las actividades encomendadas por el gerente	Todas aquellas que la sean autorizadas a ejecutar por del Gerente general
Director **RR-HH**	Ejecutar políticas de Personal Reclutamiento y selección de personal Administración de contratos, prestaciones Coordinar programas de capacitación	Todas aquellas que la sean autorizadas a ejecutar por del Gerente general
Director **Administrativo** **Financiero**	Administración de recursos Administración de materiales Vigilar el trabajo administrativo financiero Salvaguardar los recursos financieros se encarga del control administrativo	Todas aquellas que la sean autorizadas a ejecutar por del Gerente general

3. Procesos

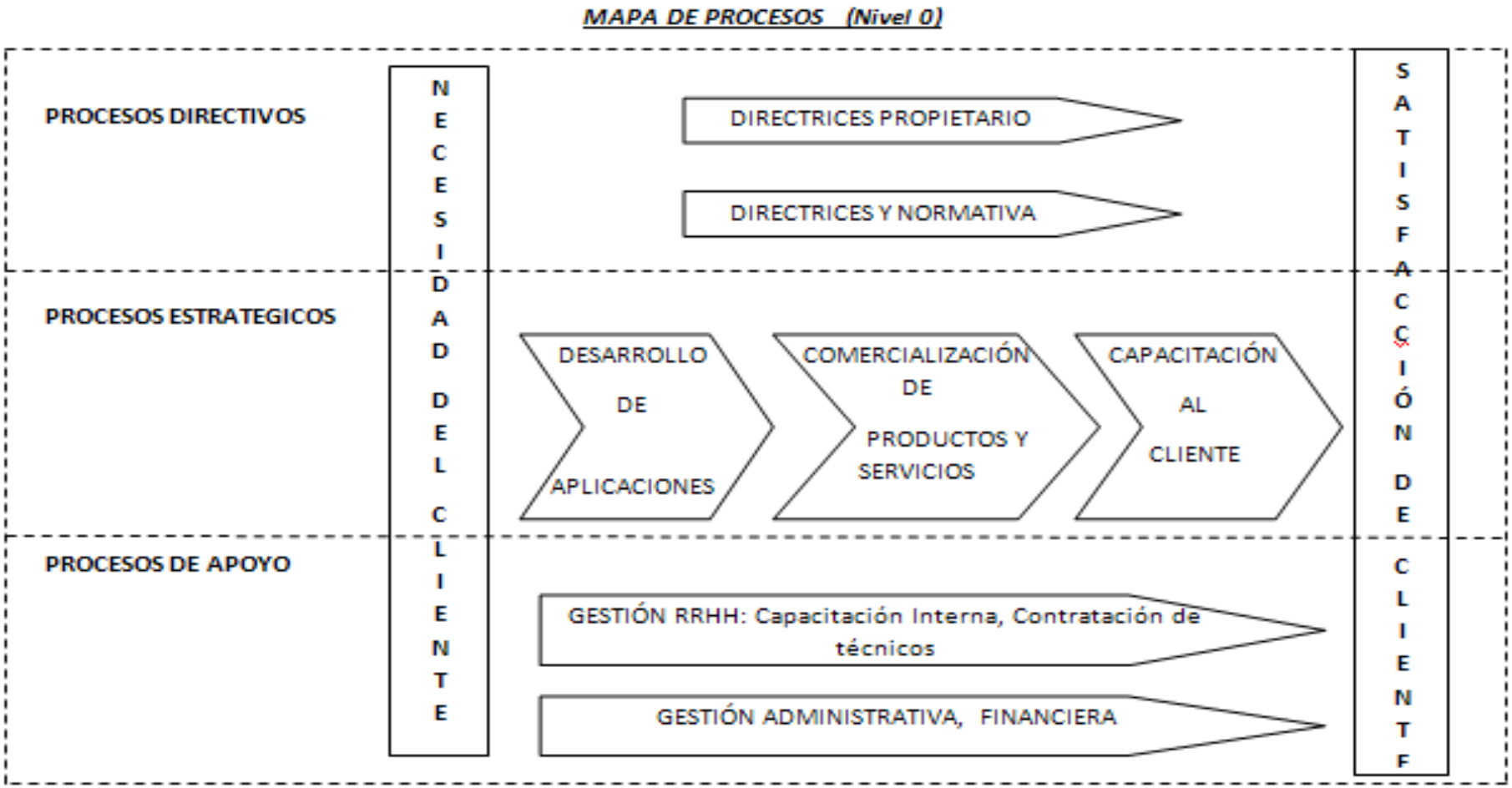
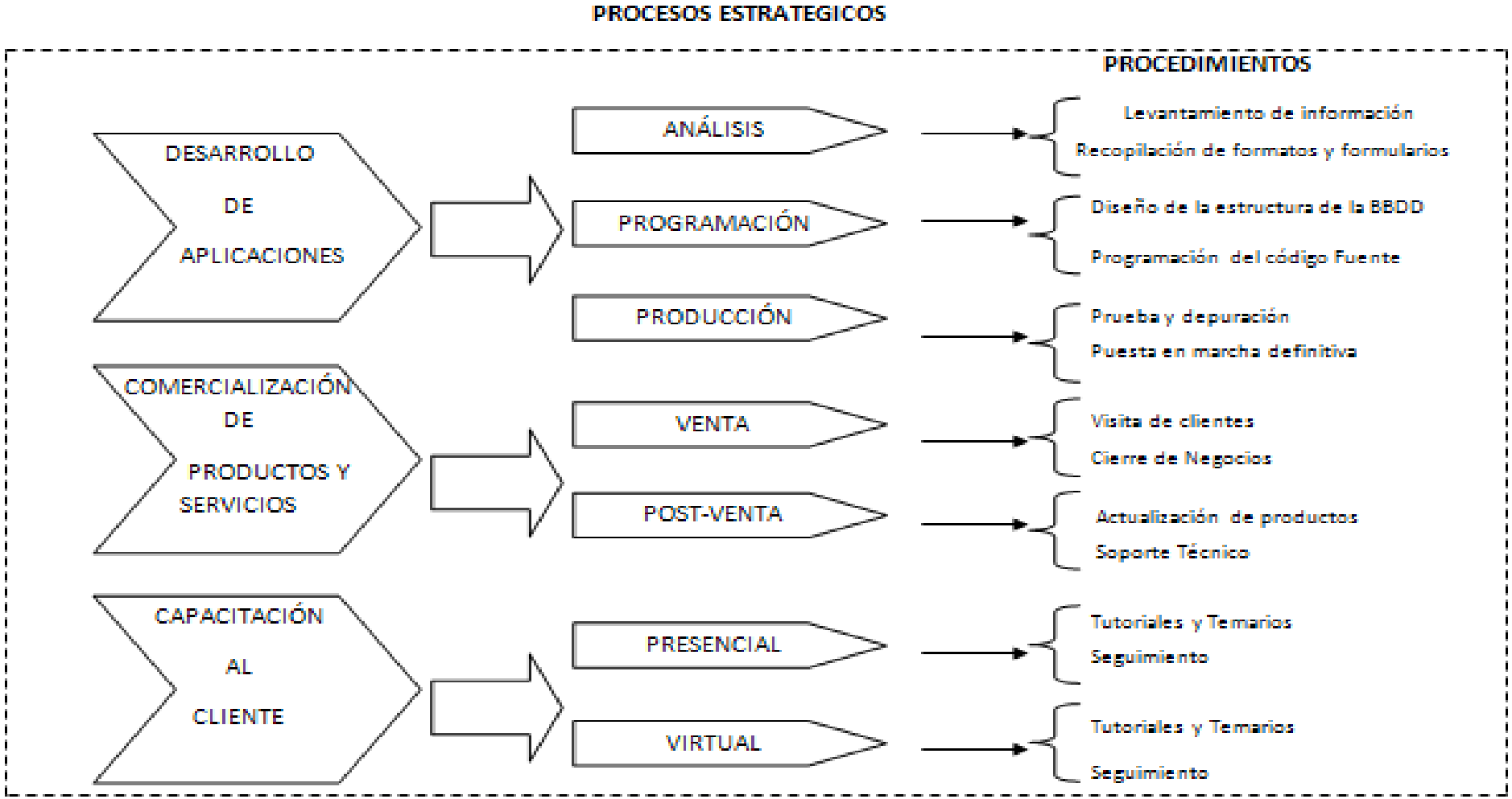


Figura # 15. Mapa de procesos propuesto para LST Nivel 0



Figura#16. Procedimientos propuestos para LST

Se distinguen tres tipos de procesos:

1. **PROCESOS DIRECTIVOS**
2. **PROCESOS ESTRATÉGICOS**
3. **PROCESOS DE APOYO**

4. Procedimientos Recomendados

PROCESOS ESTRATÉGICOS

- **DESARROLLO DE APLICACIONES**
  - **ANÁLISIS**
    - **Levantamiento de información**
      - Recopilación de datos
      - Recopilación de información
      - Identificar problemas iniciales
      - Oportunidades de mejora.

Se la realiza mediante el uso de una serie de instrumentos y técnicas como:

- Entrevistas
- Encuestas
- Observaciones Simulación
- Técnicas Audiovisuales y de inspección
    - **Recopilación de formatos y formularios**
      - Investigación de tipos de formatos y formularios
      - Revisión de formatos y formularios
      - Elección de formatos y formularios
  - **PROGRAMACIÓN**
    - **Diseño de la estructura de la BBDD**
      - Familiarización con tablas, formularios, etc.
      - Introducción de datos
      - Búsqueda y reemplazo de datos
      - Ejecución de consultas.

Según las necesidades de nuestros clientes elaboramos un diseño de la estructura de la BBDD tomando en cuenta las siguientes consideraciones:

- El tamaño de la información,
- El tipo de la información,
- Facilidad de acceso a la información,
- Facilidad para extraer la información requerida,
- El comportamiento del manejador de bases de datos con cada tipo de información

    - **Programación del código Fuente**
        - Programación inicial
        - Pruebas cortas
        - Limpieza de programación
  - **PRODUCCIÓN**
    - **Prueba y depuración**
        - Obtención de el programa ejecutable
        - Prueba a final
        - Proceso de depuración, en caso de existir errores
    - **Puesta en marcha definitiva**
        - Finalización del producto
- **COMERCIALIZACIÓN DE PRODUCTOS Y SERVICIOS**
  - **VENTA**
    - **Visita de clientes**
        - Búsqueda de clientes Potenciales
        - Fidelización de clientes
    - **Cierre de Negocios**
        - Ofertas
        - Promociones
  - **POST-VENTA**
    - **Actualización de productos**
        - Corrección de algún error
        - Observación de en que se puede mejorar
        - Realización de cambios
    - **Soporte Técnico**
        - Mantenimiento preventivo y correctivo
        - Instalación de Programas de Actualización.

        - Análisis, diagnósticos y sugerencias para mejorar un equipo informático
        - Recuperación de datos
        - Instalación de componentes adicionales
- **CAPACITACIÓN AL CLIENTE**
    - **PRESENCIAL**
        - **Tutoriales y Temarios**
            - Diseño de metodología
            - Elaboración de material
        - **Seguimiento**
            - Evaluación
            - Proceso de Seguimiento
    - **VIRTUAL**
        - **Tutoriales y Temarios**
            - Diseño de metodología
            - Elaboración de material
        - **Seguimiento**
            - Evaluación
            - Proceso de Seguimiento

4.1. Requisitos generales

4.2 Requisitos de la documentación

4.2.1. Control de Documentos

Los documentos que la Norma marca como obligatorios en todo SGSI son los siguientes:

- Alcance del SGC. (Descrito en el punto 1.2 del presente Manual de Calidad)
- Política del SGC. (Descrita en el punto 5.3 del presente Manual de Calidad)
- Objetivos de calidad. (Descritos en el punto 5.3 del presente Manual de Calidad)
- Mapa de Procesos de la Empresa. (Mostrado en la figura 12, del presente Manual de Calidad)

- Autorización y compromiso por escrito de la Dirección con el SGC. (Descrito en el punto 5.4.1 del presente Manual de Calidad.)

4.2.2 Control de los Registros

El control de registros se lo realiza en LST de la siguiente manera:

El Gerente de LST es la única persona encargada de controlar los documentos y registros utilizados en la organización.

Lo realiza de la siguiente forma:

- Revisa y actualiza documentos y registros vigentes
- Integra y actualiza las carpetas electrónicas de documentos y registros
- Actualiza documentos y registros en el portal
- Actualiza cambios en documentos y registros
- Verifica en las áreas el uso correcto de documentos y registros

5. Responsabilidad de la Dirección

5.1 Compromiso de la Dirección

Una vez iniciado el proceso de implementación de la presente normativa, que deriva en un sistema de gestión de la calidad, Todo el grupo de dirigentes que conformamos LST, nos comprometemos con el desarrollo, la implantación y la mejora del sistema establecido, y esto lo aremos:

a) Con la participación en el Consejo Asesor.
b) Internamente a través de boletines internos.
c) Promoviendo los “martes de calidad”, reunión donde la Organización discute temas relacionados con calidad.
d) Promoviendo la creación y funcionamiento del Comité de Calidad.

e) Gestionando la provisión de recursos económicos y todo lo necesario, a través del presupuesto anual de LST.[20]

5.2 Enfoque al cliente

El trabajo realizado en LST se considera está enfocando al cliente porque, se realizan las siguientes actividades:

a) Ayuda a la solución de problemas
b) Guía, dirige y propone opciones para el correcto desarrollo empresarial
c) Crea espacios para intercambio de experiencias u opiniones.
d) Brinda cursos de capacitación interna y externa.

5.3 Política de Calidad

La política de calidad de LST es la siguiente:

Figura#17. Política de Calidad de LST.

5.4 Planificación

5.4.1 Objetivos de calidad

[20] Texto desarrollado conjuntamente con los directivos de la mencionada organización

Los objetivos de calidad en LST son:

- Atender los requerimientos de todos nuestros clientes mediante procesos cada vez más ágiles y dinámicos.

- Lograr que cada uno de nuestros clientes y empleados cuenten con la capacitación y herramientas necesarias para el cumplimiento de sus respectivas actividades.

- Controlar y verificar el cumplimiento de los estándares de calidad e indicadores de gestión.

5.4.2 Planificación del Sistema de Gestión de Calidad

La Planificación del Sistema de Gestión de Calidad es consistente con la Política y los Objetivos de Calidad.

La integridad del Sistema de Gestión de Calidad se mantendrá durante la Planificación y cambios dentro del Manual de Calidad.

La Planificación del Sistema de Gestión de Calidad, es realizada por es estudiante que propone el tema para su tesis, la cual será revisada por un Comité de Calidad que deberá existir en LST.

Y se la realizara punto por punto siguiendo ordenadamente los requisitos de la norma ISO 9001

5.5. Responsabilidad, Autoridad y Comunicación

5.5.1 Responsabilidad y Autoridad

La responsabilidad y autoridad del SGC recaerá en el Comité de Calidad.

El comité de calidad deberá constar de al menos dos personas, que conozcan de calidad y auditoria el coordinador de calidad y el representante de calidad.

Estas dos personas, cada un periodo no mayor a seis meses deberán estar a cargo de revisar:

- No conformidades que hayan surgido
- Acciones preventivas o correctivas
- Formatos o documentos que requieren modificación.
- Auditorías internas y los resultados de ellas.

5.5.2 Representante de la Alta Dirección

El Gerente de LST acepta la propuesta del SGC, con las siguientes responsabilidades hacia la persona que lo propone:

- Asegurarse de que el Sistema de Gestión de Calidad sea propuesto de acuerdo con la Norma ISO 9001:2008.

- Informar a LST acerca del desempeño del SGC y de cualquier necesidad de mejora.

- Asegurar que se promueva la toma de conciencia para satisfacer los requisitos del cliente..

Asimismo, tendrá la autoridad para:

- Autorizar cambios en el MC y en los procedimientos requeridos por la Norma ISO 9001:2008

- Revisar los avances del SGC y los mecanismos de mejora continua, así como su vigencia.

5.5.3 Comunicación Interna

LST promueve la comunicación interna y la toma de conciencia sobre la importancia de las actividades de cada miembro de la organización, y de cómo contribuyen al logro de sus Objetivos, con el fin de hacer de LST una organización competitiva dentro del mercado.

5.6 Revisión por la Dirección

5.6.1 Generalidades

El Comité de Calidad, revisara el funcionamiento del SGC cuando crea necesario.
Los registros de las revisiones hechas al SGC por parte del Comité de Calidad, estarán constituidos por actas de reuniones, donde constan los resultados de la revisión.

5.6.2 Información para la Revisión

La información de entrada para llevar a cabo las reuniones de revisión por los Comités de Calidad de LST incluye:

- Resultados de las auditorías internas y externas.(Adjunto **en Anexo8**)
- Los registros de retroalimentación del cliente. (**no se cuenta con documentos, pero se lo tiene de forma mental.**)
- El desempeño de los procesos y conformidad del servicio**.(**Mediante el mapa de procesos, y con los resultados de encuestas de satisfacción del cliente Adjuntos en **Anexo 8**)
- El estado de las acciones correctivas y preventivas que se registran de acuerdo con el procedimiento, Acciones correctivas y Preventivas (**NO APLICA)** debido a que no se cuenta con este estado.
- El seguimiento de acciones y acuerdos de revisiones previas efectuadas por el Comité de Calidad de LST, que aparecen en las respectivas minutas de las reuniones. (**NO APLICA**) debido a que no se cuenta con este seguimiento.

- Los cambios sugeridos por el personal involucrado en los procesos, que puedan afectar al SGC. (**NO APLICA**) debido a que o se han sugerido cambios.

Luego de la investigación de entrada se determino qué:

LST se encontraba lejos de cumplir con los requisitos que conforman la norma ISO 27001: bebido a que:

a. Carecían de un Sistema que Gestión de Seguridad de la Información en la organización
b. No se contaba con métodos que ofrezcan seguridad en la operación y el control de los procesos que se desempeñan dentro de LST.
c. No contaban con un Manual, política y objetivos de Seguridad.
d. Aunque se tenía en mente la seguridad, no existía un compromiso formal por parte de la Dirección para fomentar, mantener y mejorar la Seguridad.
e. Carecían de un representante encargado de los aspectos de Seguridad dentro de la organización
f. No contaba con revisiones periódicas de Seguridad
g. No contaban con instrumentos que ayuden a mejorar la seguridad dentro de la organización

5.6.3 Salidas para la Revisión

Referente a los siguientes puntos:

- **La mejora de la eficacia del SGC y sus procesos.**
  Se propuso diferentes cambios en el mapa de procesos para mejorar la gestión de la calidad de los productos y servicios que ofrece LST Logística y Servicios Tecnológicos, pero fueron rechazados debido a que se menciono que el desenvolvimiento actual de la empresa se encuentra bien con el modelo de mapa de procesos que disponen.

- **La mejora del servicio en relación con los requisitos del cliente.**

Lo veremos en las **acciones correctivas** luego de revisar las evaluaciones de medición de la satisfacción del cliente

- **Las necesidades de recursos.**
  Por lo analizado en las encuestas y lo observado dentro del desenvolvimiento de la empresa puedo decir que se necesitan los siguientes recursos.

  - Por lo menos una persona que se encargue del marketing de la empresa (publicidad y ventas)

  - Intentar conseguir un Hosting propio debido a que al momento cuentan con el HOST MONSTER de 300 Gb que se lo alquila desde Francia, y por lo investigado este hosting es muy bueno, pero es recomendado para pequeñas empresas, y por lo que sabemos LST con el paso del tiempo va creciendo más y más en el mercado.

6. Gestión de Recursos

6.1 Provisión de Recursos

Los recursos requeridos por el presente manual para la propuesta de la implantación, mantenimiento y mejoramiento de la eficacia de los procesos de LST, al igual que los recursos necesarios para asegurar continuamente la satisfacción de las necesidades de los clientes serán planificados y provistos en el presupuesto anual del trabajo que se desempeña día a día.

6.2 Competencia, toma de conciencia y formación

Para la calificación, toma de conciencia y formación:
Los directivos, aseguran que el personal está consciente de la relevancia e importancia de sus actividades y con ellas contribuyen a la consecución de los objetivos de la calidad

Para el cumplimiento de este punto, LST desempeña el proceso de CAPACITACIÓN el cual en un periodo no mayor a seis meses, todo el personal de LST es formado en capacitaciones que van de acuerdo al desempeño de sus funciones.

6.3 Infraestructura

LST de acuerdo a su Presupuesto de Ingresos y Egresos, determina el suministro de recursos y la infraestructura necesaria para lograr la conformidad de clientes y empleados.

En la actualidad LST cuenta con:

a) Edificios, espacio de trabajo y servicios asociados,
   - Oficina de aproximadamente 50 m2

b) Equipo para los procesos (tanto hardware como software)

Hardware

3 PCs para desarrollo
5 PCs para desarrollo de software
2PCs para departamento administrativo

- **7 PCs TOTAL**

- Servidor Host Monster Alquilado 300gb desde Francia

Software

- De Financiamiento
- Pagina Web
- Excel (Indicadores)
- Biblioteca digital con más de 1000 libros técnicos

c) Servicios de apoyo (tales como transporte, comunicación o sistemas de información).

Enlace Internet (Punto Net)
Red de Datos Wireless / Cable

6.4 Ambiente de trabajo

Las áreas involucradas en los procesos que forman parte del alcance del SGC establecen, evalúan y propician la mejora del ambiente de trabajo necesario para lograr la conformidad con los requisitos del personal y los clientes.

Se vio la necesidad de establecer la aplicación de una encuesta para medir el ambiente de trabajo. (***Documento Adjunto en Anexo 7***)

7. Provisión del Producto

7.1 Planificación de la provisión del producto

Se realizara la actividad de planificación en los Procesos desempeñados por LST.

7.2 Procesos relacionados con el Cliente

7.2.2 Revisión de los requisitos relacionados con el producto

Los requisitos relacionados con el producto, se verifican en cada uno de los proceso de elaboración del producto que maneja LST (El cual se encuentra establecido en el mapa de procesos)

7.2.3 Comunicación con el cliente

LST buscara siempre tener contacto y buena relación con sus clientes es por eso que se ha elaborado e implantado un instrumento para conocer la satisfacción del cliente (Encuesta de medición de la satisfacción del cliente, *Documento Adjunto en* ***Anexo 4***), la cual se aplicará anualmente como tiempo máximo, para conocer como se deberá manejar y en que se está fallando, con respecto a la satisfacción del cliente.

7.3 Diseño y Desarrollo

Estos dos puntos se los maneja dentro de LST con mucha normalidad, mediante los diseños y desarrollos propios de la Organización, con nuestro proceso llamado:

- Desarrollo de aplicaciones

7.4 Compras

7.4.1 Proceso de compras

Es responsabilidad de la Dirección, que los productos adquiridos, cumplan con los requisitos de compras específicos.

Proceso actual de compras de LST

Las compras se realizan:

- De acuerdo a la necesidad
- Conforme lo necesita el cliente

} 80 %

- De acuerdo a la planificación de crecimiento } 20 %

Los Proveedores con los que se trabaja son:

- IDC
- XPC
- Tecno Mega
- COMPUMAS (Suministros)

Se propone un proceso de compras que podría resultar favorable para LST, que se encuentra Adjunto en el ***Anexo5***

Además se adjunta cuestionario para determinar el mejor proveedor *(*Adjunto en **Anexo 6**)

7.4.2 Información de las compras

Las solicitudes de compras de bienes o materiales las realizan las áreas involucradas, aplicando el formato actual, ya antes mencionado.

La Dirección se asegurara de que los requisitos de compra sean los adecuados y específicos a través de:

- Una verificación de Requisitos
- Una investigación del producto
- Una comparación de precios (vía Internet)

7.4.3 Verificación de los productos comprados

La Dirección será la encargada de verificar que los productos comprados cumplan con los requisitos de compra y especificaciones correspondientes, así como la oportunidad en la entrega, a través de:

- Una revisión General del producto

Cuándo se identifique que el proveedor no cumpla con lo estipulado, no se recibirá el producto y se buscará otro proveedor.

7.5 Producción y provisión del servicio

7.5.1 Control de la producción y de la prestación del producto.

LST introduce este concepto a través de los siguientes procesos:

- Desarrollo de aplicaciones
- Comercialización de productos y servicios
- Capacitación al cliente

El cómo se desenvuelve cada proceso lo podemos revisar en Procedimientos de LST en el punto 4. Del presente manual de Seguridad

7.5.2 Validación de los procesos para la prestación del producto.

Esta validación no aplica a ninguno de los Procesos porque LST realiza la Verificación y Validación al producto resultante.

7.5.3 Propiedad del cliente

No aplica, debido a que LST no embodega o guarda bienes de propiedad del cliente.

7.5.4 Preservación del producto

LST preservara el producto durante el proceso interno, ensamblaje, manipulación, entrega y mientras este sea utilizado por nuestros clientes.

7.6 Control de los dispositivos de seguimiento y de medición

No aplica, debido a que LST en este momento no cuenta con dispositivos de seguimiento y de medición.

Pero por este motivo se ha propuesto encuestas de medición de satisfacción del cliente y de medición del clima laboral ya antes mencionadas.

8. Medición, análisis y mejora

8.1 Generalidades

Los procedimientos de seguimiento, medición, análisis y mejora serán realizadas por el Comité de Calidad, de acuerdo a sus atribuciones.

8.2 Seguimiento y Medición

8.2.1 Satisfacción del cliente

El método empleado para la obtención de esta información es determinado por la medición de la satisfacción del cliente, a través de una encuesta, como se estipula en el punto 7.2.3

8.2.2 Auditoría Interna

De acuerdo al procedimiento de ***(Auditoría Interna Adjunto en Anexo3)***

8.2.3 Seguimiento y medición de los procesos

El Comité de Calidad se reunirá periódicamente para analizar los resultados obtenidos y se tomarán acciones correctivas, según sea necesario, para asegurar la conformidad del desempeño de los procesos.

8.2.4 Seguimiento y medición del producto

LST hará un seguimiento de las características del producto para verificar que se cumplen los requisitos del mismo. Esta verificación la deberá efectuar en el proceso de **Desarrollo de aplicaciones**

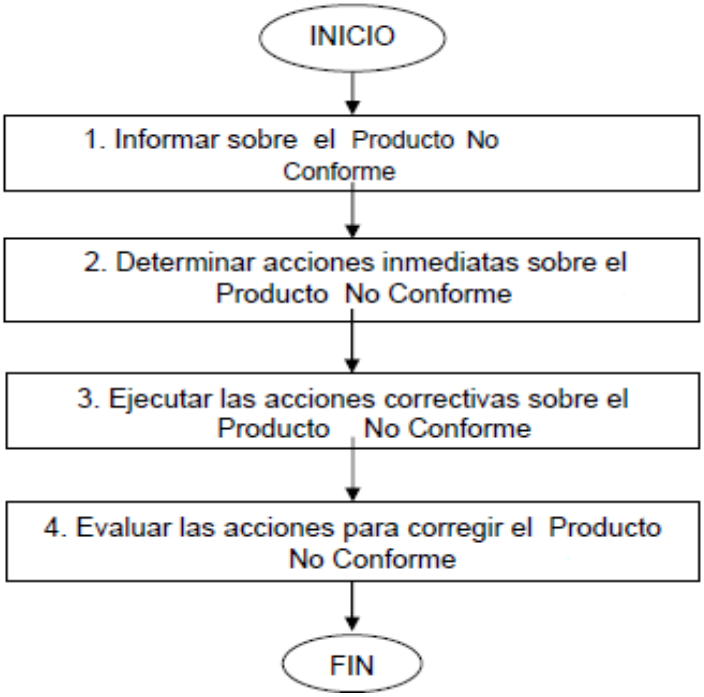
La liberación del producto se lleva a cabo hasta que se apliquen las disposiciones planificadas, a menos que la Alta Dirección apruebe ó dispense alguna de ellas.

8.3 Control del producto no conforme

Se definirá como producto no conforme al producto proporcionado por LST que no posea la calidad especificada para los mismos y/o den lugar a incumplimientos del presente Manual.

Los procesos en LST proporcionaran productos que serán utilizados en procesos posteriores que darán lugar a otros productos y así sucesivamente.

El control del producto no conforme se lo maneja de la siguiente forma:



Figura#18. Proceso de producto No Conforme de LST.

8.4 Análisis de datos

Se determinará, recopilará y analizará los datos apropiados para demostrar la eficacia del sistema y para evaluar dónde puede realizarse la mejora continua del mismo.

El resultado del análisis de los datos se presentara en las reuniones de revisión por parte de la Alta Dirección, y en cada proceso, el análisis proporciona información sobre:

- La satisfacción del cliente.
- La conformidad con los requisitos del servicio y la posibilidad de tomar acciones preventivas.
- Las características y tendencias de los procesos y servicios, incluyendo las oportunidades para llevar a cabo acciones preventivas.
- Los proveedores.

Con la inclusión de estos datos se determinará la eficacia del Sistema de Gestión de Calidad.

Con los resultados del análisis de datos se elaborará el diagnóstico para la mejora de la eficacia global del SGC, que podrá incluir la oportunidad de realizar acciones preventivas.

Este punto se lo realizó siguiendo las instrucciones debidas de la norma ISO 9001, y con esto se pudo realizar las debidas acciones preventivas y correctivas, descritas en los ítems siguientes.

8.5 Mejora

8.5.1 Mejora continua

La alta Dirección y el comité de calidad, mejorarán continuamente la eficacia del SGC, basándose en el análisis de la política de calidad, los objetivos de la calidad, los resultados de las auditorías, las revisiones de la alta dirección, el análisis de datos, las acciones correctivas y preventivas realizadas.

8.5.2 Acción correctiva

Según lo analizado y observado dentro de LST

- Por lo que se pudo observar, en LST se maneja un servidor alquilado, es por eso que se debería implementar un servidor hosting propio para brindar más seguridad y mayores ganancias a LST

- Se trato de proponer un mapa de procesos diferente al que se tiene, que pretendía obtener mejores resultados en cuanto a eficiencia de procesos, pero LST me informo que sería una pérdida de tiempo, debido les va muy bien con el mapa de procesos que se desenvuelven actualmente. (Es por eso que veremos una propuesta de mapa de procesos en las acciones Correctivas)

- Por lo investigado dentro de LST se concluyó que el proceso de desarrollo de software está dando buenos resultados, pero lo que sí está fallando es la falta de contratos o pedidos, por lo que se recomienda contratar otra persona para el departamento de marketing y ventas que tenga mucho conocimiento y experiencia en el tema, para poder obtener nuevos contratos.

Según resultados de las encuestas de:

1. **Satisfacción del cliente**

Según las encuestas de la medición de la satisfacción del cliente, podemos determinar qué:

- Los clientes dan importancia a todas características relacionadas a la calidad del servicio que presta LST (Elementos Tangibles, Fiabilidad, Capacidad de Respuesta, Seguridad, Empatía), pero se tiene cierto grado de preferencia en lo que son: Fiabilidad y seguridad.

- Definitivamente se tiene que corregir lo que son los elementos tangibles de la organización (Instalaciones Físicas, Equipos, Personal y Materiales de Comunicación) debido a que en todas las encuestas realizadas se proporciona una calificación baja en cuanto a estos elementos.

- Mejorar en cuanto a la **Capacidad de Respuesta** (Disposición, Voluntad para Proporcionar un Servicio de forma oportuna) debido a ciertos clientes que admitieron no haber recibido su producto en el tiempo establecido.

- Seguir con esa actitud de brindar un buen servicio de forma amable y respetuosa y ganándose la confianza del cliente, ya que casi todos los encuestados determinan que es así como se los trata dentro de LST

2. Ambiente Laboral

El ambiente laboral dentro de LST funciona de forma normal, según lo encuestado, los empleados dicen:

- Llevarse bien
- Estar a gusto con su trabajo
- Tener un buen trato
- Estar de acuerdo con sus remuneraciones

Pero se pudo notar que se encuentran en desacuerdo en ciertos puntos como:

- No contar con un espacio adecuado para el desenvolvimiento de sus roles
- El escaso material para el desenvolvimiento de sus tares
- La infraestructura anticuada e inadecuada.

Nota: Estos puntos deben ser corregidos a la mayor brevedad posible, si se desea que sus empleados se desenvuelvan a un 100 % dentro de la organización.

8.5.3 Acción preventiva

Por lo investigado dentro de LST se pudo llegar a proponer las siguientes acciones preventivas:

- Se propone un pequeño cambio para el actual mapa de procesos con el LST labora, debido a que en la actualidad este modelo de procesos ha estado funcionando de excelente manera, sin embargo, para la proposición del actual mapa, se modifico solamente en ciertos puntos, con el fin que no se encuentren con problemas en el transcurso del tiempo.(Estos cambios los podemos observar en el mapa de procesos propuesto para LST en la **figura#12**)

- El Host Monster que utilizan podría llegar a producir alguna perdida, ya que este Host es recomendado para empresas pequeñas y como sabemos LST crece constantemente, por eso se recomienda implementar un servidor propio.

- Sembrar un ambiente laboral más tranquilo, en lo que a infraestructura respecta, ya que por las encuestas realizadas de la medición del clima laboral nos podemos dar cuenta de que no todos los empleados están contentos con el espacio y la infraestructura necesaria para laborar en un ambiente tranquilo, y para que esto más adelante no cause problemas serios, se debería en estos momentos corregir estos problemas.

4.2 **Modelo de Gestión de la seguridad de la Información, En base a la Norma ISO 27001**

Manual de Seguridad

En base a:

Certificación ISO 27001

Para:

1. Alcance

1.1. General

El sistema de Gestión para la Seguridad de la información para LST abarca todas las áreas que corresponden al mapa de procesos de LST necesarios para garantizar la disponibilidad de los productos y servicios que ofrecen, de esta manera poder asegurar la disponibilidad de los servicios, pero sin desmejora de cualquier otra dimensión de la seguridad como lo son la integridad y la confidencialidad.

1.2. Aplicación

Para el desarrollo de este manual se hará énfasis en aquellos procesos que, por su valor a la disponibilidad de los servicios y por su susceptibilidad a sufrir riesgos de seguridad, puedan comprometer la misión de LST.

2. Referencias normativas

El sistema de gestión de Seguridad, ISO 27001:2005.

3. Términos y definiciones

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información, en adición también de otras propiedades como autenticación, autorización, registro de actividad, no repudio y confiabilidad pueden ser también consideradas.

Eventos de seguridad de la información: Ocurrencia de un evento identificado sobre un sistema, servicio o red, cuyo estado indica una posible brecha en la política de seguridad de la información o fallo en el almacenamiento de la misma, también cualquier situación previa desconocida que pueda ser relevante desde el punto de vista de la seguridad.

Incidente de seguridad: uno o varios eventos de seguridad de la información, no deseados o inesperados que tienen una cierta probabilidad de comprometer las operaciones de la empresa y amenazan a la seguridad de la información.

SGSI. El Sistema de Gestión de Seguridad de la información ayuda a establecer políticas, procedimientos y controles en relación a los objetivos del negocio de la organización**,** con el objeto de mantener siempre el riesgo por debajo del nivel asumible de la propia organización.

Evaluación de Riesgo. La evaluación de riesgos identifica las amenazas, vulnerabilidades y riesgos de la información, sobre la plataforma tecnológica de una organización, con el fin de generar un plan de implementación de los controles que aseguren un ambiente informático seguro, bajo los criterios de disponibilidad, confidencialidad e integridad de la información.

Integridad: Propiedad de salvaguardar la precisión y completitud de los recursos.

Aceptación de riesgo: Decisión de aceptar un riesgo.

Análisis de riego: Uso sistemático de la información para identificar fuentes y estimar riesgos.

Valoración de riesgo: Totalidad de los procesos de análisis y evaluación de riesgo.

Evaluación de riesgo: Proceso de comparar los riesgos estimados contra los criterios de riesgo establecidos o dados, para determinar el grado de significativo del riesgo.

4. Sistema de gestión de seguridad de la información

La conformación del SGSI de LST surge del procedimiento metodológico descrito a continuación.

Debido al interés de una persona de proponer un modelo de gestión en base a la norma ISO 27001 partiendo de la lógica que para ofrecer Productos y servicios a los Clientes, Beneficiarios y Usuarios, es necesario implementar un SGSI.

Esta propuesta fue organizada y analizada por el grupo de dirigentes con el que cuenta LST, y se llega a la conclusión de que sea propuesto, con el fin de ayudar a que LST no tenga exceso de problemas en cuanto a la seguridad de la información, además que brinde confianza y seguridad a todos sus clientes.

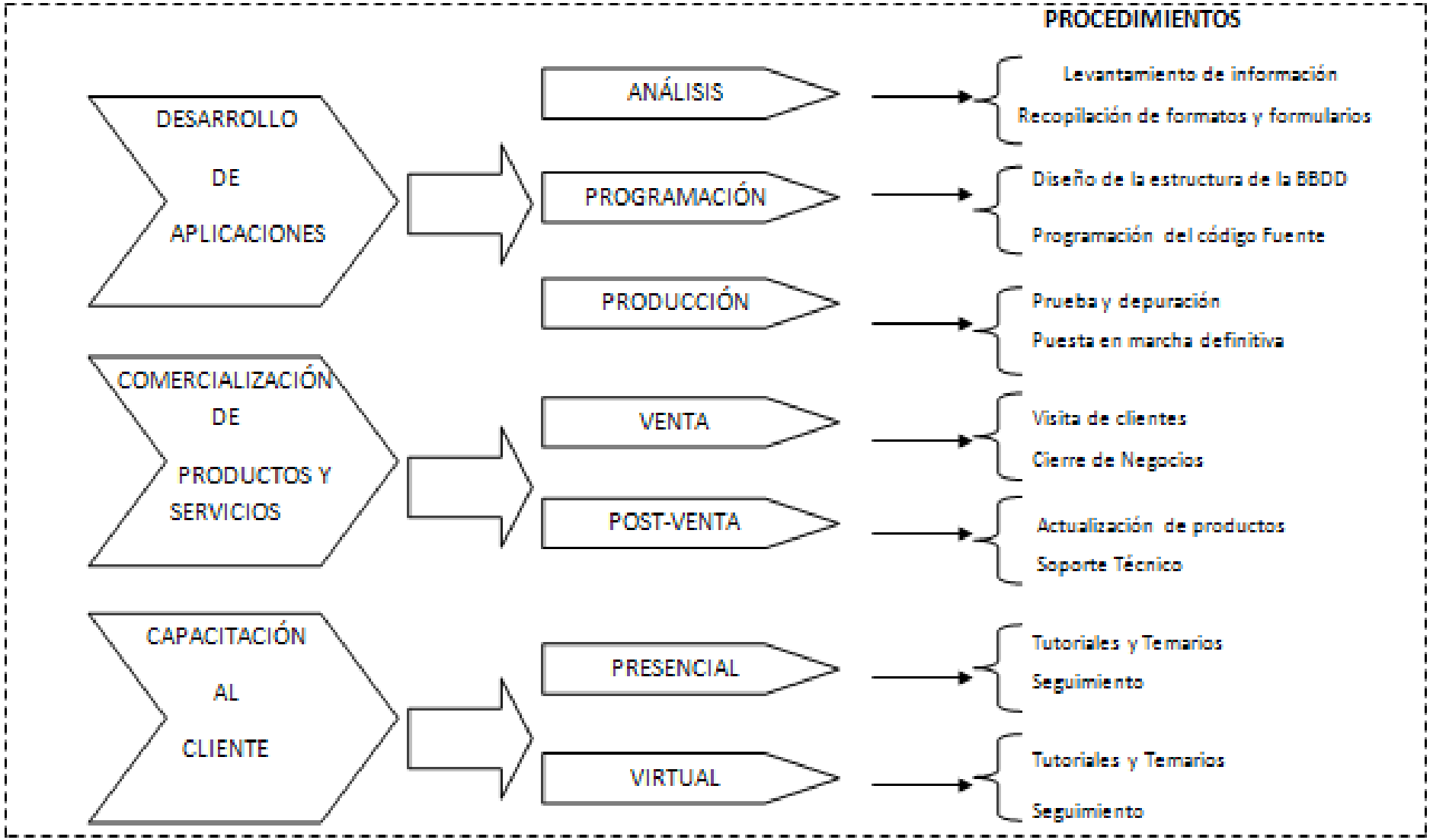
4.1. Requerimientos generales

a. Descripción de Procesos

Los procesos que se tiene en la Organización son:

1. DIRECTRICES PROPIETARIO
2. DIRECTRICES Y NORMATIVA
3. DESARROLLO DE APLICACIONES
4. COMERCIALIZACIÓN DE PRODUCTOS Y SERVICIOS
5. CAPACITACIÓN AL CLIENTE
6. GESTIÓN RRHH
7. GESTIÓN ADMINISTRATIVA, FINANCIERA

PROCESOS ESTRATEGICOS



4.2. Establecer y manejar el SGSI

4.2.1. Establecer el SGSI

4.2.1.1. Metodología de análisis de riesgo

A continuación haremos una descripción de los pasos con que contara la metodología de análisis de riesgo para LST, la cual consideramos el punto central de la definición de una estrategia de seguridad.

Determinación de la probabilidad.

La probabilidad que una vulnerabilidad potencial pueda ser explotada por una fuente de amenaza la podemos clasificar en alta, media-alta, media, media-baja y baja, como se describe a continuación:

Nivel	Definición
Alta = 5	La amenaza está altamente motivada y es suficientemente capaz de llevarse a cabo.
Media-Alta =4	La amenaza está fundamentada y es posible.
Media = 3	La amenaza es posible.
Media-Baja = 2	La amenaza no posee la suficiente capacidad.
Baja = 1	La amenaza no posee la suficiente motivación y capacidad.

Figura #19. Probabilidad de ocurrencia de un evento determinado.

De esta manera se define una escala en la cual, a una probabilidad alta, le asignamos el valor P=5, para una probabilidad media le asignamos el valor P=3 y por último para una probabilidad baja le asignamos el valor P=1, esta asignación se define en proporción directa al número de veces que el evento puede ocurrir en un periodo de un año.

Para el caso P=5 se considera que ocurre al menos dos veces al año.

Evaluación de Riesgo

No	Plataforma	División	Amenaza de Riesgo	Calificación				
				1	2	3	4	5
1	Seguridad Física	1.1 Monitoreo Ambiental	Espacio Físico			X		
			Iluminación			X		
			Niveles de humedad en Paredes					X
			Niveles Techo en mal estado					X
		1.2 Control de Acceso	Los empleados no entran a todos lados				X	
			Método adecuado para ingreso a LST			X		
			Puertas, ventanas, etc. seguras				X	
		1.3 Desastres Naturales	Inundación			X		
			Erupción volcánica			X		
			Terremoto				X	
		1.4 Control de Incendios	Materiales para combatir incendio				X	
			Instalaciones eléctricas adecuadas				X	
2	Conexiones a Internet	2.1 Políticas en el Firewall	Falla Firewall en hardware			X		
			Falla de Firewall en software			X		
		2.2 Detección de intrusos	No poseer el indicado			X		
			Caducidad			X		
3	Infraestructura de comunicaciones	3.1 Routers	No poseer quien lo administre				X	
			Muy antiguos			X		
		3.2 Switches	Problemas con Switches				X	

	3.3 Hubs	Problemas con Hubs				X	
	3.4 Servidores	No contar con servidor propio					X
		Poca capacidad de almacenamiento				X	
4 Sistema Operacional	4.1 Respaldos	No contar con respaldos					X
	4.2 Tiempo de recuperación	Demasiado demorado				X	
5 Correo Electrónico	5.1 Soporte	Des configuración de cuentas					X
		Problemas al comunicarse con servidor				X	X

Identificación de Vulnerabilidades.

Tomaremos en cuenta las amenazas de nivel 5 ya que estas son las que se deben corregir con la mayor brevedad posible, debido a que son las amenazas que están altamente motivas y son suficientemente capaces de llevar a cabo; y son los siguientes:

Monitoreo Ambiental

- Niveles de humedad en Paredes (Todas las paredes de las oficinas provocan un aspecto de sudoración)
- Niveles Techo en mal estado (Parte del techo de la oficina gerencial partiéndose y filtrando agua)

Servidores

- No cuentan con servidor propio

Respaldos

- No cuentan con respaldos

Soporte (Correo electrónico)

- Desconfiguración de cuentas del correo electrónico
- Problemas al comunicarse con servidor al momento de la utilización del correo electrónico

4.2.2. Implementar y operar el SGSI

Básicamente, la implantación de un SGSI se reduce a las siguientes acciones:

TRATAMIENTO DE RIESGO

- Se recomienda reparar techo y paredes, ya que se encuentran en mal estado, y esto podría perjudicar la seguridad de la información

- Se recomienda implementar un servidor propio debido a que al momento cuentan con uno alquilado y por lo investigado este hosting, es muy bueno pero es recomendado para pequeñas empresas, y por lo que

sabemos LST con el paso del tiempo va creciendo más y más en el mercado

- Se recomienda a la mayor brevedad diseñar una política y/o procedimientos de respaldo, debido a que por las encuestas hechas de la seguridad de la información en años pasados existieron muchas pérdidas debido a este problema.

- Se recomienda tener cuidado con los problemas que pueden presentarse en el correo electrónico, ya que los problemas de LST se podría deber a los problemas más comunes, los mismos que describimos a continuación

- Está conectado a Internet o a una red, o el servidor de correo no está disponible temporalmente.
- La configuración de cuenta no es correcta.
- Su perfil de usuario está dañado.
- Un elemento de correo electrónico del servidor está dañado.
- La configuración del software antivirus no es correcta.
- Se ha quitado del equipo o la instalación está dañada.
- La configuración del software de firewall personal no es correcta.

4.2.3. Mantener y mejorar el SGSI

Para mantener y mejorar el SGSI la gerencia se compromete a cumplir con los siguientes puntos:

a) La Implementación de las mejoras identificadas en el SGSI y asegurar que las mejoras logren sus objetivos señalados.

b) La Toma de acciones correctivas y preventivas apropiadas

c) La comunicación de los resultados y acciones

4.3. Requerimientos de documentación

4.3.1. General

Requisitos de Documentación

Toda la documentación generada por el SGSI debe ser aprobada por la Dirección antes de proceder a su distribución formal en la organización.

4.3.2. Control de documentos

Los documentos que la Norma marca como obligatorios en todo SGSI son los siguientes:

- Alcance del SGSI. (Descrito en el punto 1 del Manual de Seguridad de la información)
- Objetivos de Seguridad de la Información

OBJETIVOS

  - Mantener la Integridad, Confidencialidad y Disponibilidad en lo que a Seguridad de la información se refiere.
  - Evitar los problemas de violación de información, que se han venido viviendo en anteriores años.
  - Garantizar que el material y los recursos de software se usen únicamente para los propósitos para los que fueron creados.

- Política del SGSI.

POLÍTICA DE SEGURIDAD DEL SGSI

LST Logística y Servicios Tecnológicos, es una empresa dedicada a aportar soluciones tecnológicas a las empresas mediante la implementación de software.

Conscientes de la importancia que la seguridad de la información

tiene para el desarrollo de su negocio ha decido que se proponga un sistema de gestión y la presente política.

LST Logística y Servicios Tecnológicos, establece, define y revisa unos objetivos dentro de su Sistema de Gestión de Seguridad de la Información (Descritos en el punto anterior.) encaminados a mejorar su seguridad, entendiéndola como la conservación de la confidencialidad, disponibilidad e integridad de su información, aumentando la confianza de sus clientes y otras partes interesadas.

El diseño, implantación y mantenimiento del SGSI se apoyará en los resultados de un proceso continuo de análisis y gestión de riesgos del que se derivan las actuaciones a desarrollar en materia de seguridad dentro del alcance de su sistema que es la “Gestión de la Seguridad de la Información en el diseño, el desarrollo, la implementación y el mantenimiento de sistemas informáticos.

La Dirección de LST Logística y Servicios Tecnológicos revisara los criterios de evaluación del riesgo propuestos de manera que todos aquellos escenarios que impliquen un nivel de riesgo inaceptable sean tratados adecuadamente.

Como parte del SGSI, cuando sea implementado, la Dirección desarrollará, implantará y mantendrá actualizado un Plan de Continuidad de Negocio acorde a las necesidades de la empresa y dimensionado a los riesgos que le afectan.

La Dirección de LST Logística y Servicios Tecnológicos se comprometerá a la implantación, mantenimiento y mejora del SGSI dotándolo de aquellos medios y recursos que sean necesarios y motivando a todo el personal para que asuma este compromiso.

La presente política será de aplicación a todo el personal y recursos que se encuentran dentro del alcance del SGSI, se pone en su

conocimiento y es comunicada a todas las partes interesadas.

El Gerente
Ing. Eduardo Sierra

- Evaluación de riesgos. (Descrito en el punto 4.2.1.1 del presente manual de Calidad)
- Informe del Análisis de Riesgos. (Descrito en el punto 4.2.2 del presente manual de Calidad)
- Autorización y compromiso por escrito de la Dirección con el SGSI. (Descrito en el punto 5.1 del Manual de seguridad.)
- Procedimientos, que aseguren la efectiva planificación, operación y control de los procesos de seguridad del SGSI. (Todo englobado en el manual de seguridad)

4.3.3. Control de registros

El control de registros se lo describe en el punto 4.2.2 del Manual de Calidad:

5. Responsabilidad de la gerencia

5.1. Compromiso de la gerencia

Cuando se llegue a implementar este proyecto en nuestra empresa, Todo el grupo de dirigentes que conformamos LST, nos comprometemos con el desarrollo, la implantación y la mejora del Sistema de Gestión de Seguridad establecido, y esto lo aremos:

- Con la participación en el Consejo Asesor.
- Internamente, a través de boletines.
- Promoviendo reuniones donde la Organización discuta temas relacionados con seguridad.
- Promover la creación y funcionamiento de un Comité de Seguridad.
- Gestionar la provisión de recursos económicos e infraestructura a través del presupuesto anual de LST.

5.2. Gestión de recursos

5.2.1. Provisión de recursos

La organización está de acuerdo en determinar y proporcionar los recursos necesarios para cumplir con todos los puntos que se establecen en la norma ISO 27001:

5.2.2. Capacitación, conocimiento y capacidad

La organización se asegurará que todo el personal sea competente para realizar las tareas requeridas por la Norma ISO 27001.

La organización también se asegurará que todo el personal relevante esté consciente de la relevancia e importancia de sus actividades de seguridad de la información y cómo ellos pueden contribuir al logro de los objetivos SGSI.

6. Auditorías internas SGSI

De acuerdo al procedimiento de ***(Auditoría Interna*** *Adjunto en* ***Anexo3)***

7. Revisión Gerencial del SGSI

7.1. General

La gerencia revisará el SGSI de la organización a intervalos planeados (por lo menos una vez al año) para asegurarse de su continua idoneidad, conveniencia y efectividad. Esta revisión debe incluir oportunidades de evaluación para el mejoramiento y la necesidad de cambios en el SGSI, incluyendo la política de seguridad y los objetivos de seguridad de la información. Los resultados de las revisiones deberán documentarse claramente.

7.2. Insumo de la revisión

Luego de haber investigado y evaluado a LST se puede decir que esta organización se encontraba lejos de cumplir con los requisitos que conforman la norma ISO 9001:2008: bebido a que:

a. Carecía de un Sistema que Gestión de Calidad en la organización

b. No se contaba con métodos que aseguren la operación y el control de los procesos que conforman un Sistema de Gestión de la Calidad
c. No contaban con un Manual, política y objetivos de calidad.
d. Aunque se tenía en mente la calidad, no existía un compromiso formal por parte de la Dirección para fomentar, mantener y mejorar la Calidad.
e. Carecían de un representante encargado de los aspectos de calidad dentro de la organización
f. No contaba con revisiones periódicas de Calidad
g. A pesar de que tienen bien identificados los recursos y proveedores principales de la organización, no cuentan con un método tal que identifique y proporcione lo indispensables para la implantación, mantenimiento y mejora de la efectividad de la Calidad.
h. No contaban con instrumentos de medición de la satisfacción del cliente, como la del clima laboral.

7.3. Resultado de la revisión

- Todos los puntos con los que no contaba LST fueron analizados y elaborados con el fin de hacer esta propuesta de implementación del Sistema de Gestión de Seguridad de la Información SGSI, basado en la norma ISO 27001, con el fin de mejorar la seguridad de la información, dentro de LST.

- Debemos tener en cuenta que la implantación de un SGSI es un proceso largo y complejo, que si no es gestionado correctamente desde el inicio, puede conllevar unos gastos incrementados y la posibilidad de fracaso.

- Sin embargo, los mismos factores que pueden hacer fracasar este tipo de proyecto, administrados con especial cuidado, pueden convertirse en lo que esperamos, ventajas que hagan un proyecto más sencillo de realizar y gestionar, con gastos coherentes.

- Se elaboró una ***Encuesta de Seguridad*** que se encuentra **adjunta en el Anexo9** para conocer el estado en el que se encontraba LST,

con respecto a la seguridad de la información.

- Además se elaboro el Análisis de Riesgo de LST que se encuentra en el punto EVALUACIÓN DE RIESGO dentro del manual de Seguridad de la Información**,** con el fin de determinar cuáles son las falencias que se deben corregir con mayor brevedad para una mejor seguridad de la información.

8. Mejoramiento del SGSI

La implantación del SGSI debe ser un proceso dinámico. A estas alturas ha debido quedar claro que la misión del SGSI es situar la seguridad de la información al mismo nivel que cualquier otro objetivo de negocio, y como tal, debe ser optimizado continuamente.

Es por esto que se corrigieron todos los literales que se describieron en el punto 7.2 del manual de seguridad.

8.1. Mejoramiento contínuo

La alta Dirección y el encargado que ellos determinen, serán responsables de mejorar continuamente la eficacia del SGSI, basándose en el análisis de la política de seguridad, los resultados de las auditorías, las revisiones de la alta dirección, el análisis de datos, las acciones correctivas y preventivas realizadas.

8.2. Acción correctiva

Estas acciones correctivas etas descritas en el análisis de riesgo (tratamiento de riesgo) descrito en el punto **4.2.2** del manual de seguridad.

8.3. Acción preventiva

Luego de analizar el método de seguridad de la información de LST me he podido dar cuenta de que la hace falta una herramienta especializada que se encargue de identificar vulnerabilidades en los sistemas operativos, y debido a investigaciones realizadas en Ecuador y en otros países se ha llegado a la

conclusión que una de las mejores herramientas hoy en día en el mercado, que permite identificar vulnerabilidades es:

GFI Report Center, la cual ayudara a LST a:

- Buscar de vulnerabilidades en su red (Windows y Linux)
- Directorios compartidos, puertos abiertos, cuentas no usadas.
- Revisar actualizaciones aplicadas en los sistemas operativos.
- Detección de dispositivos USB

CAPÍTULO V

5.1. CONCLUSIONES

5.1.1. En base a norma ISO 9001

- Se pudo notar una clara diferencia entre trabajar con un modelo establecido y trabajar únicamente en base a rutina es decir sin un modelo documentado.

- Con el desarrollo del documento de calidad se pueden determinar Las áreas o procesos en los que se está cometiendo errores, y con ello buscar formas para corregirlos y lograr que su desenvolvimiento sea de manera correcta.

- Se tuvo resultados favorables en cuanto a ISO 9001, gracias al apoyo incondicional de la gerencia y de los trabajadores que en LST laboran.

- Para realizar el diseño y estructura del Sistema de Gestión de Calidad se hizo un diagnostico de la organización frente a los requerimientos de la norma ISO 9001, mediante el cual se identifico que LST estaba lejos de cumplir con los requisitos establecidos por esta norma.

5.1.2. En base a norma ISO 2700

- Al hablar acerca de normas ISO en la organización, en primera instancia, no se le dio la importancia debida, ya que la mayoría de personas no conocían el buen desempeño organizacional que estas crean, Pero ahora que ya lo conocen todos se muestran muy interesados en ellas.

- LST ha tenido serios problemas en cuanto a información es por eso se pide se tome conciencia de la importancia de la seguridad de la información, y así evitar futuros inconvenientes, incluso más graves que los que se ha tenido. Recomendación

- Lo que se busca para LST con respecto a la seguridad de la información es reducir el riesgo a niveles aceptables, ya que la seguridad absoluta no existe.

- Para realizar el modelo de gestión de seguridad de la información fue necesario contar con una política de seguridad adecuada. Esta política puso de manifiesto el compromiso de la dirección en relación a la protección de la información y estableció el marco general de seguridad para el negocio y sus objetivos.

5.2. RECOMENDACIONES

5.2.1. En base a norma ISO 9001

- Incluir en el plan de capacitación cursos relacionados a la utilización de herramientas, mejoramiento, entre otras, enfocadas a la calidad, que permitan al personal tener un nivel técnico para el buen desempeño de la calidad dentro de LST.

- Contratar de suma urgencia por lo menos una persona que se encargue del marketing de la empresa, debido a que hace falta un funcionario que dirija los contratos para publicidad y ventas; sin embargo de que LST realiza ventas, ‘estas no suficientes como las que una organización mediana y de gran importancia, debería tener.

- Implementar un servidor propio debido a que al momento cuentan con el HOST MONSTER de 300 Gb que se lo alquila desde Francia, y por lo investigado este hosting, es muy bueno pero es recomendado para pequeñas empresas, y por lo que sabemos LST con el paso del tiempo va creciendo más y más en el mercado.

5.2.2. En base a norma ISO 27001

- Se recomienda el uso sostenido de esta propuesta como una herramienta para realizar el análisis de la seguridad de la información dentro de LST, de manera que se pueda conocer cómo se está manejando y como se debería manejar correctamente la seguridad de la información en la organización.

- La propuesta debe ser considerada como un mecanismo de mejoramiento continuo y no estático, donde se implementen las mejoras identificadas en el SGSI, lo que permitirá asegurar que dichas mejoras alcancen los objetivos pretendidos

- Contar con personal clave y con las peticiones exigidas por la Norma ISO 27001 dentro de la empresa ya que esto evita la contratación de consultorías externas cuyo costo suele ser muy elevado.

- Implantar el SGSI siempre buscando objetivos claros que agreguen valor a la organización.

- Que toda nueva implementación en pro de mejoras en la seguridad de la información esté acompañado de políticas funcionales que direccionen los esfuerzos hacia los objetivos del SGSI

5.1. BIBLIOGRAFÍA

Arroyo, Luis; Brais Quirós y Murillo Gerardo. Clima organizacional y satisfacción del usuario externo, en la Sección de Sistemas de Información del Departamento de Tecnología de la Información del Poder Judicial de Costa Rica, en julio de 2007. Universidad de las Ciencias y el Arte de Costa Rica, San José Costa Rica, 2007.

ISO-IEC 27001. Information technology- security techniques – Information security management systems – requirements. 2005.

ISO-IEC 27001. Information technology- security techniques – Code of practice for information security management. 2005.

Membrana Martínez, Joaquín. Metodologías Avanzadas para la planificación y mejora. Ediciones Díaz De Santos. Madrid, 2007

Magerit versión 2: Metodología de análisis y gestión de riesgos de los sistemas de información. Ministerio de administraciones públicas de España. Madrid, 2006.

NIST. Guía de gestión del riesgo para sistemas de tecnologías de información. Departamento de Comercio de los Estados Unidos. Instituto nacional de estándares y tecnología. USA. 2001

Sánchez Garreta, José; Chalmeta Rosales, Ricardo; Collell Simón, Oscar, Monfort Manero, Pilar y Campos Sancho Cristina. Ingeniería de proyectos informáticos: actividades y procedimientos. Editorial Universitas. Valencia, España, 1998.

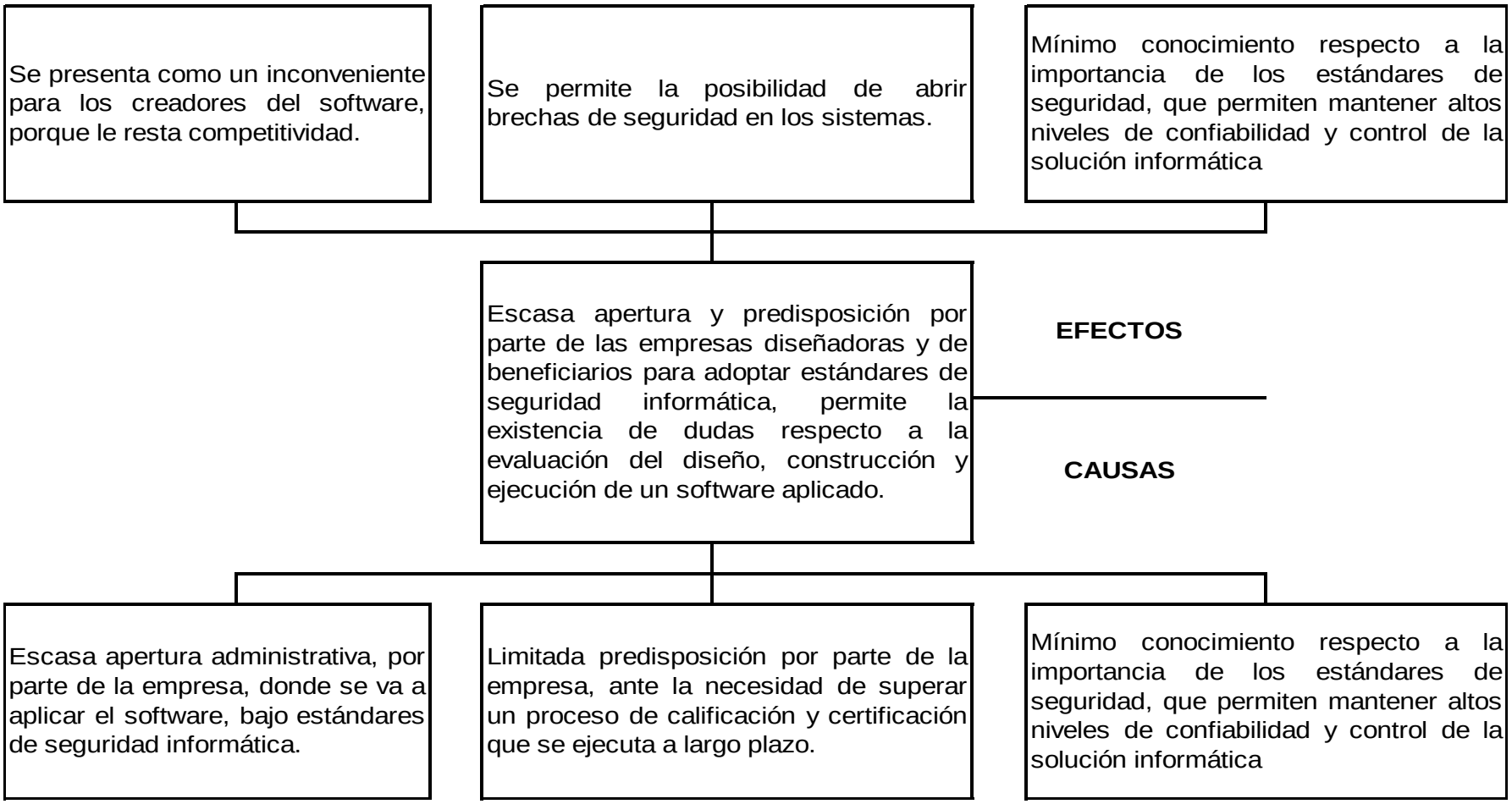
Philip B. Crosby; Completeness (Plenitud); Calidad para el siglo XXI; Líder de la Revolución de la calidad en América.

5.4. ANEXOS

5.3.1. Anexo1

ÁRBOL DE PROBLEMAS

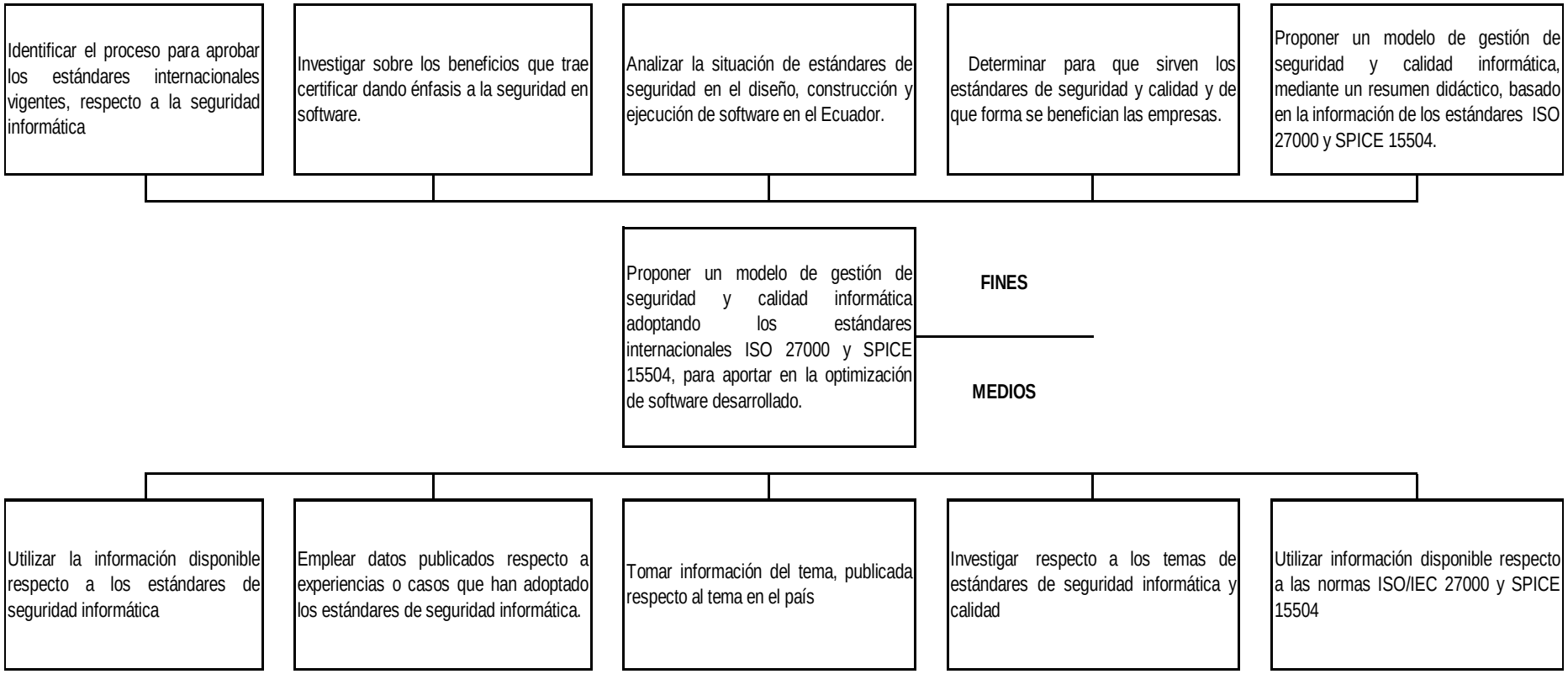
ÁRBOL DE PROBLEMAS



5.3.2. Anexo2

ÁRBOL DE OBJETIVOS

ÁRBOL DE OBJETIVOS



5.3.3. Anexo 3

Procedimiento de Auditorías Internas

1. Objetivo

- Diseñar el procedimiento para realizar una Auditoría Interna del Sistema de Gestión de Calidad / y el Sistema de Gestión de Seguridad con la finalidad de indicar como llevar a cabo la auditoría en la empresa LST.

- Resultado que se desea alcanzar al aplicar este procedimiento es el de obtener información que nos permita mejorar y mantener el Sistema de Gestión de Calidad / y Sistema de Gestión de Seguridad funcionando correctamente; es decir que se esté llevando a cabo para cumplir con los objetivos de Calidad y Seguridad planteados.

2. Alcance

- Se realiza una auditoría interna anualmente o dos al año en caso de ser necesario; se pueden auditar áreas específicas o todas las áreas de la fábrica en las que se aplique el Sistema de Gestión de Calidad y de Seguridad.

3. Documentos de Referencia

- Sección 8.2.2 “Auditorías Internas” del Manual de Calidad de la empresa LST.
- Sección 6 “Auditorías Internas ” del Manual de Seguridad de la empresa LST

- El plan de Auditorías Internas

4. Responsabilidades

- En el Manual de Gestión de Calidad se indica que el responsable de la auditoría interna del SGC es el Comité de Calidad, mientras que para la auditoría interna del SGSI será la propia dirigencia; quienes deberán aprobar el Plan de Auditoría Interna cada vez que esta se realice. Al aprobar el plan se asigna el Auditor Jefe y el equipo auditor; así como las secciones o áreas a auditar.

4.1. Auditor Jefe

El auditor Jefe designado está preparado para realizar correctamente la auditoría siendo una persona objetiva e imparcial; que ha sido formada y adquirido experiencia en el campo de auditorías. Tiene la responsabilidad de:

- Seleccionar al personal que será su equipo de auditores.
- Informarse adecuadamente sobre las áreas en las que se realizara la auditoría interna.
- Comunicar a los auditados, con anticipación cuando se realizara la auditoría.
- Planificar y coordinar con el equipo formado la auditoría a realizarse.
- Es el responsable de representar al equipo y presentar el informe final de la auditoría frente al Comité de Calidad y el Gerente General.

4.2. Los auditores

El personal para poder ser seleccionado para el equipo auditor debe de cumplir ciertas responsabilidades, estar capacitado y tener conocimientos sobre las Normas a auditar, sobre los Manuales de Gestión de Calidad y de Seguridad respectivamente de la empresa y sobre todo tener la formación de auditor interno. Los auditores están encargados de:

- Ser objetivo e imparcial.
- Colaborar con el Auditor Jefe en todo el proceso de la auditoria.
- Informar el motivo y forma de llevar la auditoría a los auditados.
- Prepararse adecuadamente antes de comenzar la auditoría conociendo las áreas que va auditar.

4.3. El auditado

Todo auditado debe de cumplir con la responsabilidad de:

- Facilitar el acceso a las instalaciones y de los documentos pertinentes al equipo auditor.
- Cooperar con los auditores en todo lo que este a su alcance para asegurar el éxito de la Auditoría.
- Poner en marcha las acciones correctivas que se deriven del informe de Auditoría.

5. Desarrollo

- Una vez aprobado el Plan de Auditorías Internas; se deben dar diferentes pasos para el adecuado desarrollo de la auditoría de la siguiente manera.

5.1. Comunicación a los Auditados.

La auditoría debe de planificarse con dos meses de antelación, los jefes de las áreas a ser auditadas deben de estar notificados con un mes de anticipación. La comunicación es muy importante para lograr una auditoría exitosa. Las fechas y horas de la auditoría deben de acordarse con exactitud.

5.2. Planificación de la Auditoría.

Con la planificación nos referimos al nombramiento del equipo auditor y de las áreas a ser auditadas. Se define el encargado de cada área y el tiempo que se tomara a realizar la auditoría. Así como también el procedimiento y sistema que se aplicara según convenga con el área auditada.

5.3. Ejecución de la Auditoria.

Para llevar a cabo la auditoría interna del Sistema, de Calidad y de Seguridad se analiza cada departamento a auditar para determinar qué requisitos del sistema de Calidad y de Seguridad son aplicables y sobre ello desarrollar la auditoría.

El equipo auditor debe interactuar con el personal responsable de cada departamento auditado, revisando registro si el caso lo amerita. La finalidad es comprobar y verificar que el Sistema de Calidad y de Seguridad se están cumpliendo correctamente. Si se da el caso de encontrarse una desviación del sistema es declarada como No-conformidad, se deben reportar mediante un informe documentado; si existen pruebas visuales se las pueden adjuntar.

Al realizar el plan de auditoría se designan los puntos a controlar y preguntas a realizar al auditado. De esta manera él, comprueba, si se están cumpliendo con los procedimientos y obteniendo resultados según los objetivos planteados.
El auditado debe ser informado sobre las No Conformidades encontradas y sobre las conclusiones a las que se ha llegado; estas serán analizadas en la reunión de cierre con el equipo auditor

.

5.4. Informe de la Auditoria.

En la reunión de cierre se realiza el informe de la Auditoría el responsable del mismo es el Jefe Auditor. El informe se lo dirige al Comité de Calidad, al Gerente General y a los responsables de cada área que se auditó.

Este informe reúne los datos sobre las evidencias encontradas en las diferentes áreas; se pueden determinar cómo No Conformidades leves, medias o críticas; aunque también se pueden reportar simples observaciones. Si el equipo auditor tienes evidencias objetivas y tangibles se adjuntan al reporte final.

Todo informe de auditoría incluye las recomendaciones que el equipo auditor proporciona para eliminar las causas de las No conformidades encontradas.

5.5. Seguimiento de Acciones Correctivas.

Luego de que se detectaron las No Conformidades y se entregó el informe al Gerente; se solicita que se realicen las correcciones en un tiempo determinado dependiendo del grado de cada desviación; es un documento impreso donde se acuerda el plazo acordado y se da una recomendación de cómo eliminar la causa de la No Conformidad.

El objetivo del seguimiento de acciones correctivas es el de verificar que se están tomando medidas adecuadas para eliminar la No conformidad; el Jefe Auditor hace un seguimiento a las acciones correctivas y realiza si es posible el cierra de la No Conformidad. En caso de no poder cerrar el caso se da un mínimo plazo y en el caso que no sean satisfactorias las medidas tomadas, se realiza el estudio y se analiza la posibilidad de nuevas acciones correctivas.

5.3.4. Anexo 4

MODELO DE ENCUESTA DE MEDICIÓN DE SATISFACCIÓN DEL CLIENTE

Nombre de la empresa:

Nombre del Representante:

Cargo que ocupa en la empresa:

Deseamos conocer su opinión acerca del servicio que le brinda LST

Los resultados obtenidos en las encuestas contribuirán con nuestro compromiso de atenderlo cada vez mejor.

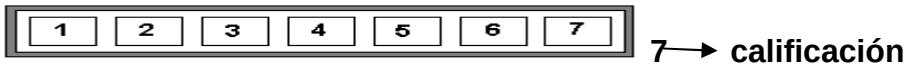
Instrucciones: Debe poner notas del 1 al 7 a cada una de las 22 preguntas que se realizan a continuación.

Opción	Decisión	Calificación
a	Total desacuerdo	1
b	Desacuerdo	2
c	En Parcial desacuerdo	3
d	Ni acuerdo, Ni desacuerdo	4
e	Poco de acuerdo	5
f	Casi de acuerdo	6
g	Total Acuerdo	7

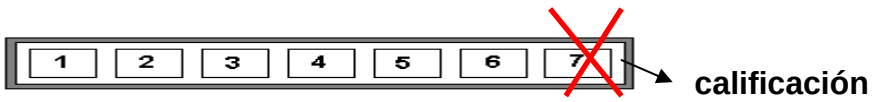
EJEMPLO:

Entendió usted la forma de calificar esta encuesta?

- Si la calificación se hace en forma digital



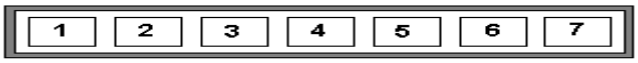
- Si la calificación se hace con esferográfico.



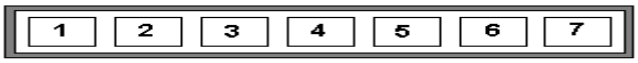
Métrica: que representa cada número

Elementos Tangibles.- (Instalaciones Físicas, Equipos, Personal y Materiales de Comunicación).

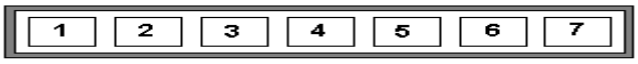
P.1 Las instalaciones físicas de LST (oficinas) son cómodas y agradables.



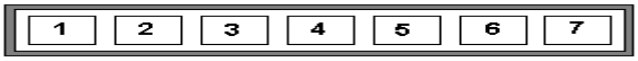
P.2 Los equipos de computación, sistemas utilizados por LST para la realización de su trámite son modernos y están actualizados.



P.3 Los empleados de LST muestran una apariencia agradable y profesional.

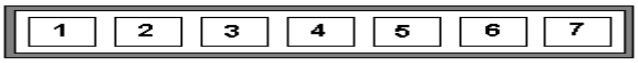


P.4 Los documentos, formularios, folletos entregados por LST para la realización de su trámite son claros, y útiles.

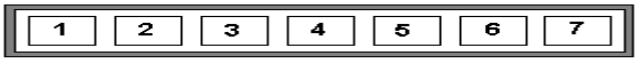


Fiabilidad.- (Habilidad para ejecutar el Servicio Prometido de forma y Cuidadosa)

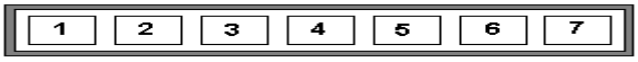
P.5 LST cumple con hacer su trámite en el tiempo prometido.



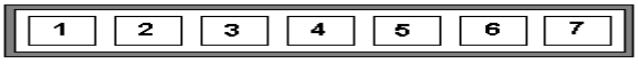
P.6 LST presta habitualmente bien sus servicios.



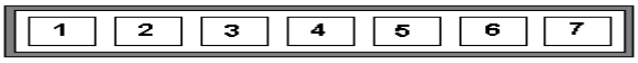
P.7 Cuando usted tiene algún tipo de inconveniente, el equipo de LST muestra interés por solucionar su problema.



P.8 LST mantiene sus registros, documentos, datos de forma segura (no hay posibilidad de que se extravíen.).

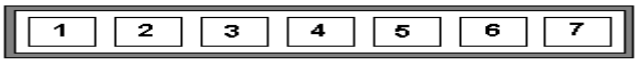


P.9 Confía en que todo el equipo de LST le atiende de forma oportuna y eficiente.

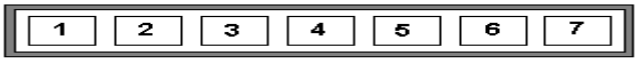


Capacidad de Respuesta.- (Disposición, Voluntad para Proporcionar un Servicio de forma oportuna).

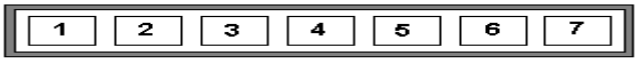
P.10 El proceso con el que fue atendido está hecho para entregarle una buena atención.



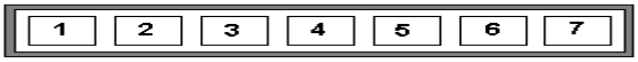
P.11 LST reacciona oportunamente a sus demandas.



P.12 El tiempo que tarda en realizar un proceso le parece adecuado

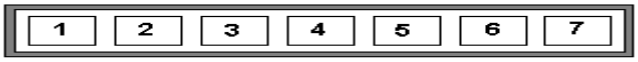


P.13 LST informa exactamente cuando las actividades relacionadas con su pedido van a ser ejecutadas.

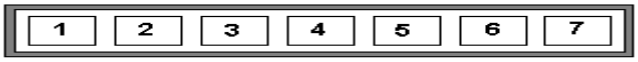


Seguridad.- (Conocimiento, Cortesía, Habilidades para Inspirar Credibilidad y Confianza).

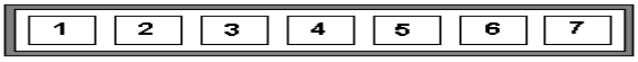
P.14 El equipo de LST está dispuesto a ayudarlo.



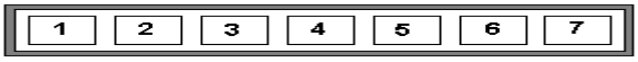
P.15 El comportamiento ético del equipo de LST transmite confianza.



P.16 Usted se siente seguro el momento de ser atendido por LST.

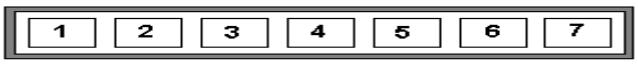


P.17 El equipo de LST es amable con usted.

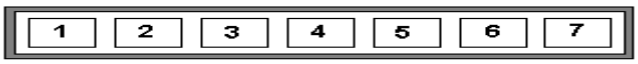


Empatía.- (Atención Individualizada)

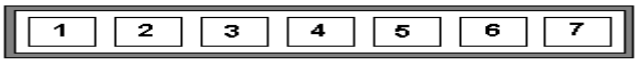
P.18 El equipo de LST tiene los conocimientos y destrezas suficientes para proporcionarle una buena atención.



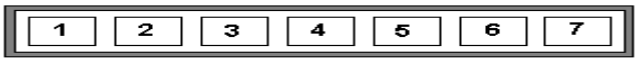
P.19 Los horarios de atención de LST son convenientes a sus intereses.



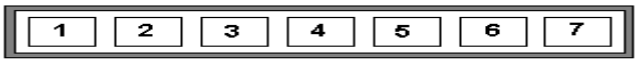
P.20 El equipo de LST tiene una amplia relación con sus clientes.



P.21 LST entiende las necesidades específicas del cliente.



P.22 LST siempre busca el beneficio del cliente.



ENCUESTA DE MEDICIÓN DE SATISFACCIÓN DEL CLIENTE

Instrucciones: En la siguiente lista aparecen 5 características relacionadas a la calidad del servicio que presta LST. Nos gustaría conocer que tan importante es cada una de estas características, para esto usted debe repartir 100 puntos entre cada una de ellas.

Nº CARACTERÍSTICAS PUNTAJE

D.1 **Elementos Tangibles:** Instalaciones Físicas, Equipos, Personal y Materiales de Comunicación).

D.2 **Fiabilidad:** Habilidad para ejecutar el Servicio Prometido de forma y Cuidadosa).

D.3 **Capacidad de Respuesta:** Disposición, Voluntad para Proporcionar un Servicio de forma oportuna).

D.4 **Seguridad.-** (Conocimiento, Cortesía, Habilidades para Inspirar Credibilidad y Confianza).

D.5 **Empatía.-** (Atención Individualizada)

T O T A L 100

Comentarios / Sugerencias

MUCHAS GRACIAS

5.4.5. Anexo 5

PROCESO DE COMPRAS

Proceso de Evaluación de Proveedores

Procedimiento

1. Búsqueda de los posibles proveedores basándose en recomendación del producto, renombre en el mercado, guías de industrias u otros datos que ayudan a seleccionarlos.

2. A los posibles proveedores se les hace llegar un Cuestionario de Selección de Proveedores (Adjunto al final del documento), en la que se solicita la información general de la compañía, así como datos de los productos y otros anotados en el formato.

3. Selección de los nuevos proveedores.

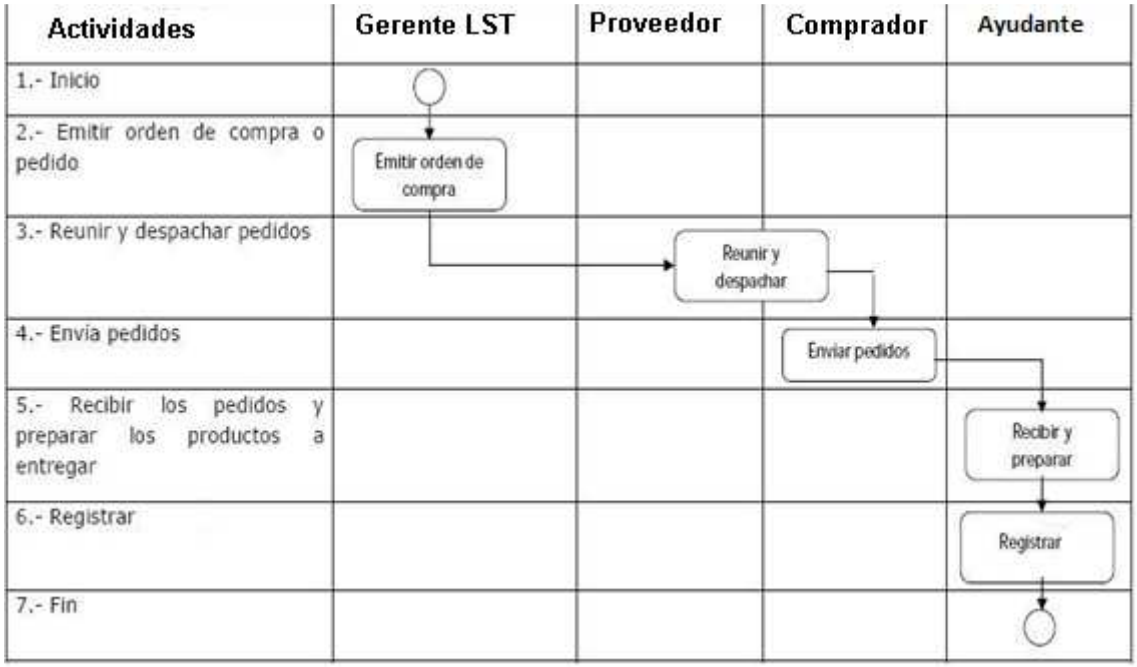
4. El proveedor seleccionado y aprobado en la evaluación es registrado en una Lista de Proveedores Aprobados

   Los proveedores se someterán a Evaluación obligatoriamente cada seis meses, ó cuando así lo creamos necesario

Registros utilizados en el proceso

- Evaluación Continua de Proveedores
- Cuestionario de Selección de Proveedores
- Lista de Proveedores Aprobados
- Evidencia de Compras

Diagrama de Proceso de Compras


Actividades
Gerente LST
Proveedor
Comprador
Ayudante
1.- Inicio
2.- Emitir orden de compra o pedido
Emitir orden de compra
3.- Reunir y despachar pedidos
Reunir y despachar
4.- Envia pedidos
Enviar pedidos
5.- Recibir los pedidos y preparar los productos a entregar
Recibir y preparar
6.- Registrar
Registrar
7.- Fin

5.3.6. Anexo 6

Cuestionario para proveedores

1. Detalles Direccion

Nombre de empresa		Número de teléfono	
Dirección de visita		Número de fax	
Código Postal		Dirección internet	
Ciudad		Correo electrónico	
Pais			

2. Persona de contacto de seguridad de producto

Nombre		Número de fax	
Cargo		Correo electrónico	
Número de teléfono		Número de teléfono fuero horario de oficina (en caso de calamidades)	

3. Mecanografíe a compañía
(seleccione qué se aplica)

☐ Comercio al por mayor ☐ Comerciante (solamente oficina)

4. Certificación del producto

¿Puede usted indicar según qué estándares se certifican los productos que usted nos proporciona?

5. **Sistema de calidad**

¿Posee su empresa un certificado de un sistema de calidad? ☐ Si ☐ No
En caso de sí, remítenos una copia del certificado.

☐ ISO

☐ Otras

6. **Ningunos certificado el sistema de calidad**

¿posee su empresa un sistema de calidad por escrito? ☐ Si ☐ No
En caso de sí, remítenos una copia del Manual de calidad

¿en este momento usted esta en fase de obtener un certificado? ☐ Si ☐ No

En caso de sí ¿que certificado?

¿Cuándo espera usted la fecha de certificación?

¿Cuáles de los siguientes actuaciones se han efectuados para garantizar la seguridad de los productos? (marca los realizados):

☐ Normas para los trabajadores, cómo:

7. ¿Los productos que usted suministran se puede hacer un seguimiento por completo? ☐ Si ☐ No

8. ¿En caso de sí, usted estará dispuesto a demostrar los resultados si le solicitamos? ☐ Si ☐ No

5.3.7. Anexo 7

MODELO DE ENCUESTA DE MEDICIÓN DEL AMBIENTE LABORAL

LST como empresa preocupada de la forma permanente por el desarrollo y satisfacción de sus empleados desea ofrecerle la posibilidad de expresar su opinión respecto a las condiciones en las que usted desempeña su trabajo.
A continuación se encuentra una serie de afirmaciones y preguntas, las cuales agradeceremos sean respondidas con la mayor sinceridad y honestidad posible marcando la alternativa que mejor describa lo que sientes o piensas.
NOTA: no existen respuestas correctas o incorrectas. Esta encuesta es anónima

1. En relación a las condiciones físicas de su puesto de trabajo (iluminación, temperatura, ventilación, espacio, volumen de ruidos, etc.) usted considera que este es

- ☐ Muy confortable
- ☐ Confortable
- ☐ Poco confortable
- ☐ Incomodo
- ☐ Muy Incomodo

2. Usted tiene el suficiente tiempo para realizar su trabajo habitual

- ☐ Siempre
- ☐ Casi siempre
- ☐ Algunas veces
- ☐ Casi nunca
- ☐ Nunca

3. Está usted de acuerdo en cómo está gestionado el departamento en el que trabaja respecto a las metas que este tiene encomendadas

- ☐ Siempre
- ☐ Casi siempre
- ☐ Algunas veces
- ☐ Casi nunca
- ☐ Nunca

4. Considera que recibe una justa retribución económica por las labores desempeñadas

- ☐ Siempre
- ☐ Casi siempre
- ☐ Algunas veces
- ☐ Casi nunca
- ☐ Nunca

5. Su jefe inmediato tiene una actitud abierta respecto a sus puntos de vista y escucha sus opiniones respecto a cómo llevar a cabo sus funciones

- ☐ Siempre
- ☐ Casi siempre
- ☐ Algunas veces
- ☐ Casi nunca
- ☐ Nunca

6. Cómo calificaría su nivel de satisfacción por trabajar en la organización

- ☐ Muy alto
- ☐ Alto
- ☐ Regular
- ☐ Bajo
- ☐ Muy bajo

7. En mi oficina se fomenta y desarrolla el trabajo en equipo

- ☐ Siempre
- ☐ Casi siempre
- ☐ Algunas veces
- ☐ Casi nunca
- ☐ Nunca

8. Para el desempeño de mis labores mi ambiente de trabajo es

- Muy malo
- Malo
- Regular
- Bueno
- Muy bueno

9. Existe comunicación dentro de mi grupo de trabajo

- Siempre
- Casi siempre
- Algunas veces
- Casi nunca
- Nunca

10. Siento que no me alcanza el tiempo para completar mi trabajo

- Siempre
- Casi siempre
- Algunas veces
- Casi nunca
- Nunca

11. Los jefes de la organización se preocupan por mantener elevado el nivel de motivación del personal

- Siempre
- Casi siempre
- Algunas veces
- Casi nunca
- Nunca

12. La relación entre compañeros de trabajo en la organización es

- Muy mala
- Mala
- Regular
- Buena
- Muy buena

13. La organización otorga buenos y equitativos beneficios a los trabajadores

- Siempre
- Casi siempre
- Algunas veces
- Casi nunca
- Nunca

14. Las remuneraciones están a nivel de los sueldos de mis colegas en el mercado

- Siempre
- Casi siempre
- Algunas veces
- Casi nunca
- Nunca

15. Siento apoyo en mi jefe cuando me encuentro en dificultades

- Siempre
- Casi siempre
- Algunas veces
- Casi nunca
- Nunca

16. Mi jefe me da autonomía para tomar las decisiones necesarias para el cumplimiento de mis responsabilidades

- Siempre
- Casi siempre
- Algunas veces
- Casi nunca
- Nunca

17. Mi jefe me proporciona información suficiente, adecuada para realizar bien mi trabajo

- Siempre
- Casi siempre
- Algunas veces
- Casi nunca
- Nunca

18. El nivel de recursos (materiales, equipos e infraestructura) con los que cuento para realizar bien mi trabajo es

- Muy mala
- Mala
- Regular
- Buena
- Muy buena

19. Los jefes reconocen y valoran mi trabajo

- Siempre
- Casi siempre
- Algunas veces
- Casi nunca
- Nunca

20. Cómo calificaría su nivel de satisfacción por pertenecer a la organización

- Muy alto
- Alto
- Regular
- Bajo
- Muy bajo

21. Te agradeceremos nos hagas llegar algunos comentarios acerca de aspectos que ayudarían a mejorar nuestro ambiente de trabajo

_____
_____
_____

5.3.8. Anexo 8

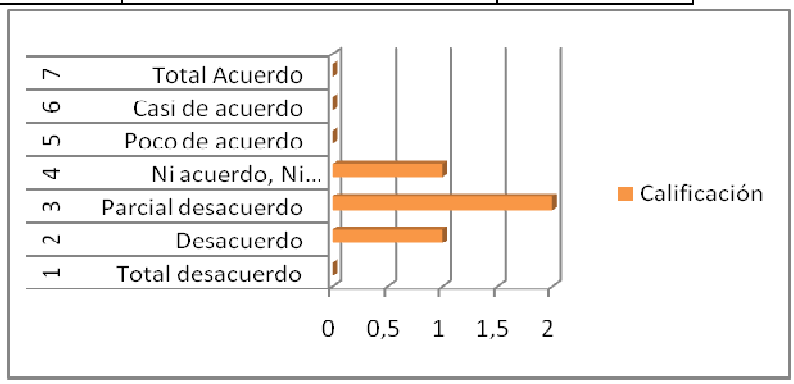
RESULTADO DE ENCUESTAS

- **Resultado de las encuestas de la medición de la satisfacción del cliente:**

Elementos Tangibles Instalaciones Físicas, Personal y Materiales de Comunicación).

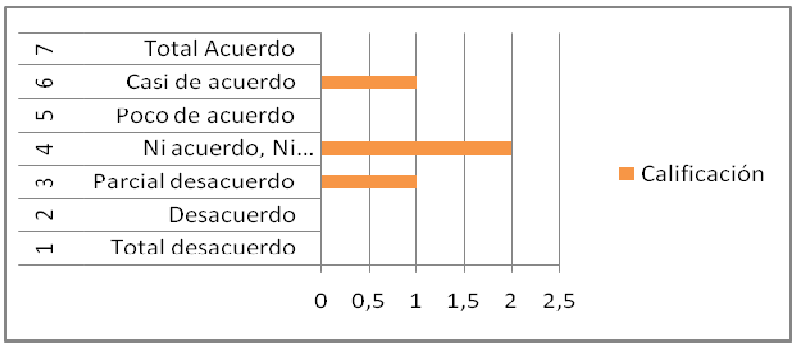
P.1 Las instalaciones físicas de LST (oficinas) son cómodas y agradables.

Nivel	Decisión	Calificación
1	Total desacuerdo	0
2	Desacuerdo	1
3	Parcial desacuerdo	2
4	Ni acuerdo, Ni desacuerdo	1
5	Poco de acuerdo	0
6	Casi de acuerdo	0
7	Total Acuerdo	0



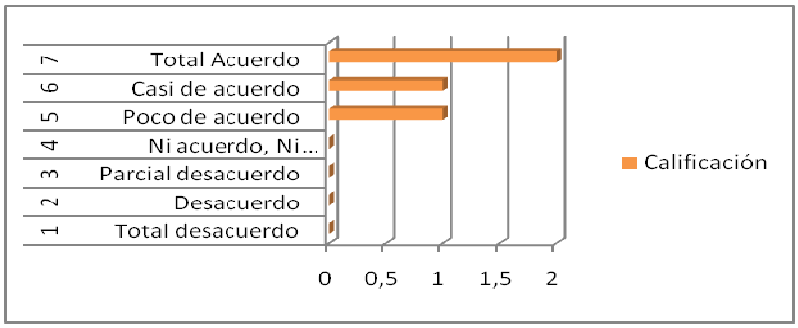
P.2 Los equipos de computación, sistemas utilizados por LST para la realización de su trámite son modernos y están actualizados

Nivel	Decisión	Calificación
1	Total desacuerdo	0
2	Desacuerdo	0
3	Parcial desacuerdo	1
4	Ni acuerdo, Ni desacuerdo	2
5	Poco de acuerdo	0
6	Casi de acuerdo	1
7	Total Acuerdo	0



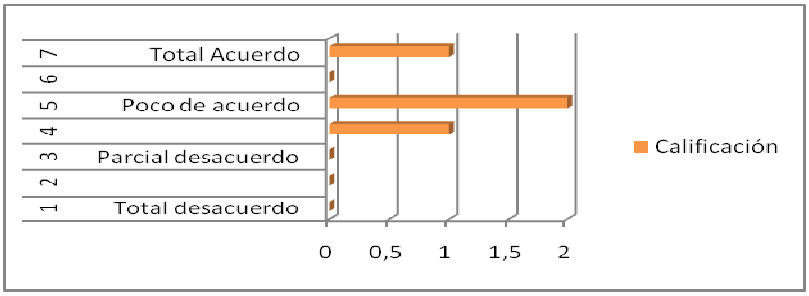
P.3 Los empleados de LST muestran una apariencia agradable y profesional.

Nivel	Decisión	Calificación
1	Total desacuerdo	0
2	Desacuerdo	0
3	Parcial desacuerdo	0
4	Ni acuerdo, Ni desacuerdo	0
5	Poco de acuerdo	1
6	Casi de acuerdo	1
7	Total Acuerdo	2



P.4 Los documentos, formularios, folletos entregados por LST para la realización de su trámite son claros y útiles.

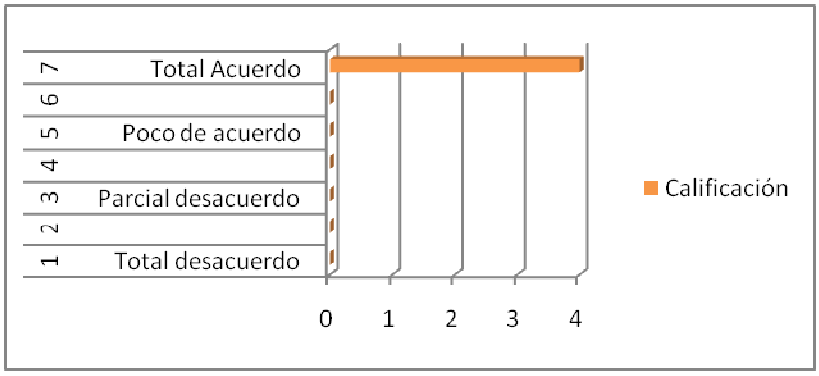
Nivel	Decisión	Calificación
1	Total desacuerdo	0
2	Desacuerdo	0
3	Parcial desacuerdo	0
4	Ni acuerdo, Ni desacuerdo	1
5	Poco de acuerdo	2
6	Casi de acuerdo	0
7	Total Acuerdo	1



Fiabilidad.- (Habilidad para ejecutar el Servicio Prometido de forma y Cuidadosa)

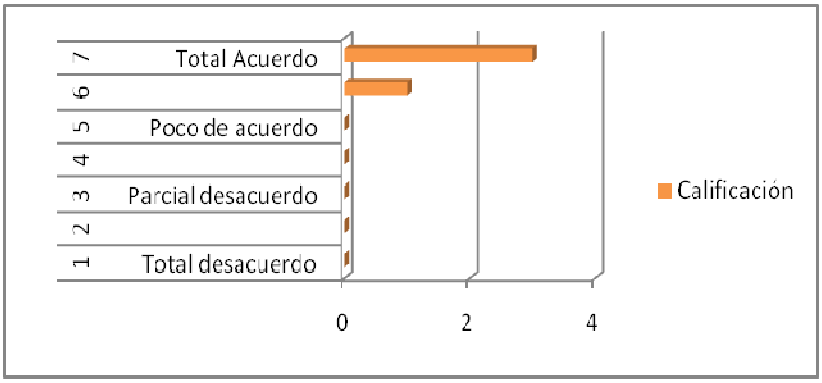
P.5 LST cumple con hacer su trámite en el tiempo prometido.

Nivel	Decisión	Calificación
1	Total desacuerdo	0
2	Desacuerdo	0
3	Parcial desacuerdo	0
4	Ni acuerdo, Ni desacuerdo	0
5	Poco de acuerdo	0
6	Casi de acuerdo	0
7	Total Acuerdo	4



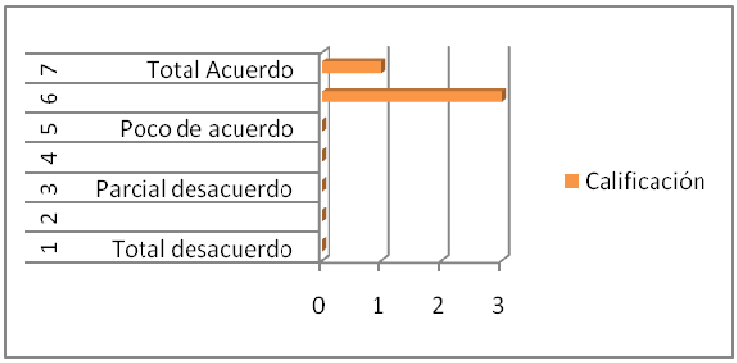
P.6 LST presta habitualmente bien sus servicios.

Nivel	Decisión	Calificación
1	Total desacuerdo	0
2	Desacuerdo	0
3	Parcial desacuerdo	0
4	Ni acuerdo, Ni desacuerdo	0
5	Poco de acuerdo	0
6	Casi de acuerdo	1
7	Total Acuerdo	3



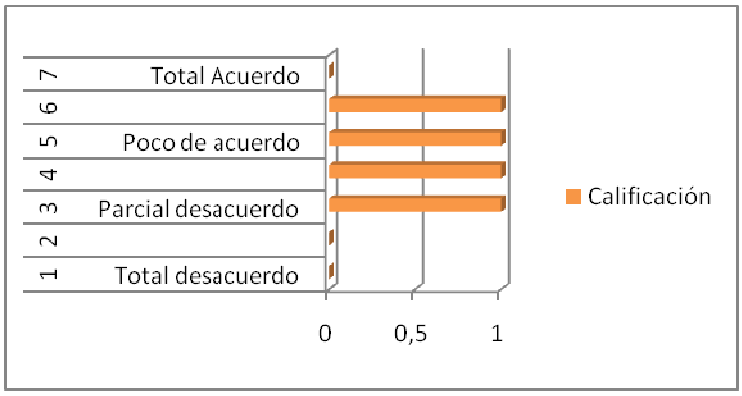
P.7 Cuando usted tiene algún tipo de inconveniente, el equipo de LST muestra interés por solucionar su problema.

Nivel	Decisión	Calificación
1	Total desacuerdo	0
2	Desacuerdo	0
3	Parcial desacuerdo	0
4	Ni acuerdo, Ni desacuerdo	0
5	Poco de acuerdo	0
6	Casi de acuerdo	3
7	Total Acuerdo	1



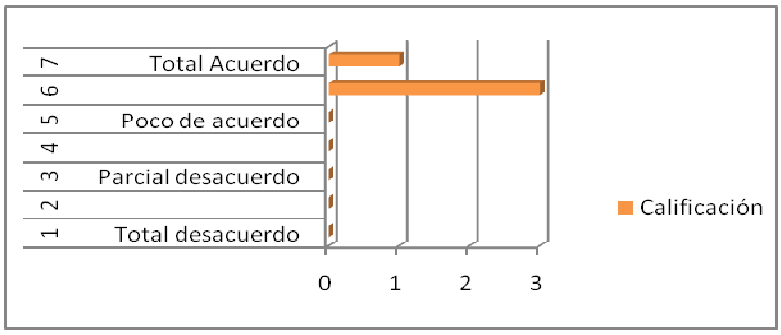
P.8 LST mantiene sus registros, documentos, datos de forma segura (no hay posibilidad de que se extravíen.)

Nivel	Decisión	Calificación
1	Total desacuerdo	0
2	Desacuerdo	0
3	Parcial desacuerdo	1
4	Ni acuerdo, Ni desacuerdo	1
5	Poco de acuerdo	1
6	Casi de acuerdo	1
7	Total Acuerdo	0



Nivel	Decisión	Calificación
1	Total desacuerdo	0
2	Desacuerdo	0
3	Parcial desacuerdo	0

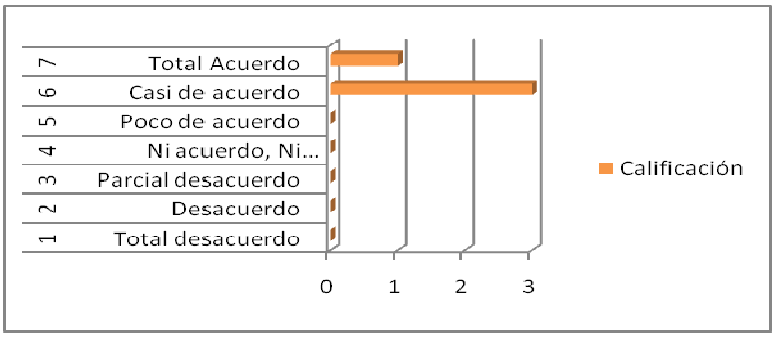
4	Ni acuerdo, Ni desacuerdo	0
5	Poco de acuerdo	0
6	Casi de acuerdo	3
7	Total Acuerdo	1



Capacidad de Respuesta.-(Disposición, Voluntad para Proporcionar un Servicio)

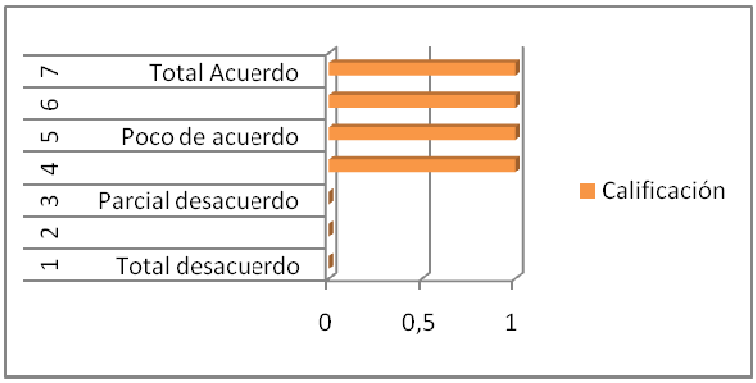
P.10 El proceso con el que fue atendido está hecho para darle una buena atención.

Nivel	Decisión	Calificación
1	Total desacuerdo	0
2	Desacuerdo	0
3	Parcial desacuerdo	0
4	Ni acuerdo, Ni desacuerdo	0
5	Poco de acuerdo	0
6	Casi de acuerdo	3
7	Total Acuerdo	1



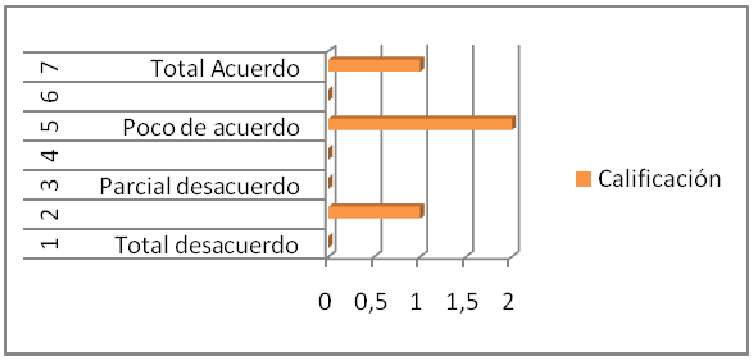
P.11 LST reacciona oportunamente a sus demandas

Nivel	Decisión	Calificación
1	Total desacuerdo	0
2	Desacuerdo	0
3	Parcial desacuerdo	0
4	Ni acuerdo, Ni desacuerdo	1
5	Poco de acuerdo	1
6	Casi de acuerdo	1
7	Total Acuerdo	1



.12 El tiempo que tarda en realizar un proceso le parece adecuado

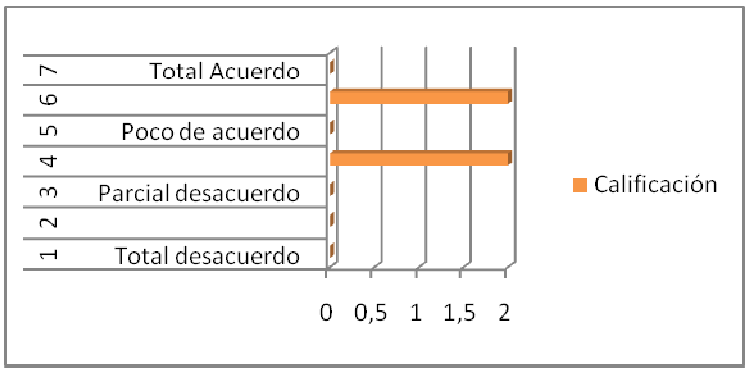
Nivel	Decisión	Calificación
1	Total desacuerdo	0
2	Desacuerdo	1
3	Parcial desacuerdo	0
4	Ni acuerdo, Ni desacuerdo	0
5	Poco de acuerdo	2
6	Casi de acuerdo	0
7	Total Acuerdo	1



P.13 LST informa exactamente cuando las actividades relacionadas con su pedido

van a ser ejecutadas

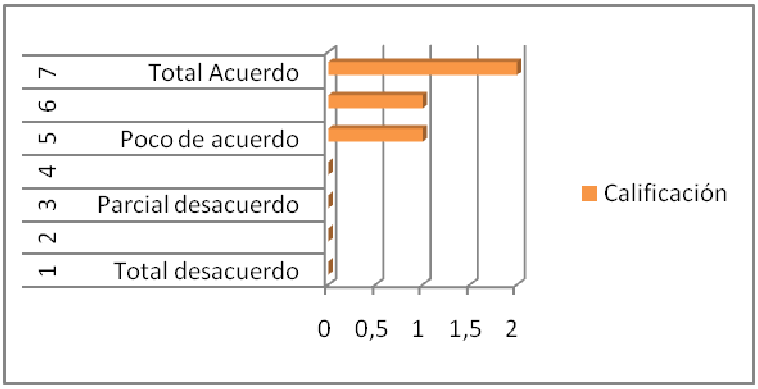
Nivel	Decisión	Calificación
1	Total desacuerdo	0
2	Desacuerdo	0
3	Parcial desacuerdo	0
4	Ni acuerdo, Ni desacuerdo	2
5	Poco de acuerdo	0
6	Casi de acuerdo	2
7	Total Acuerdo	0



Seguridad.- (Conocimiento, Cortesía, Habilidades para Inspirar Credibilidad y confianza).

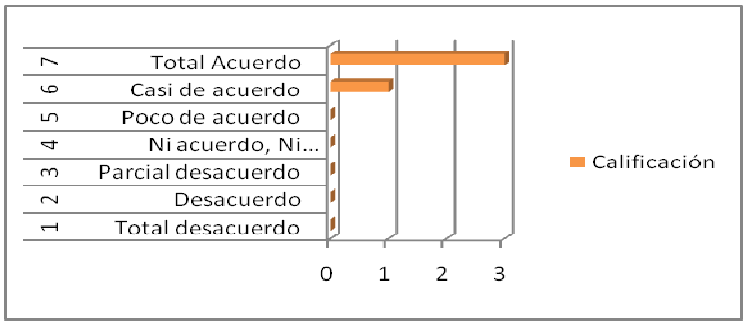
P.14 El equipo de LST está dispuesto a ayudarlo.

Nivel	Decisión	Calificación
1	Total desacuerdo	0
2	Desacuerdo	0
3	Parcial desacuerdo	0
4	Ni acuerdo, Ni desacuerdo	0
5	Poco de acuerdo	1
6	Casi de acuerdo	1
7	Total Acuerdo	2



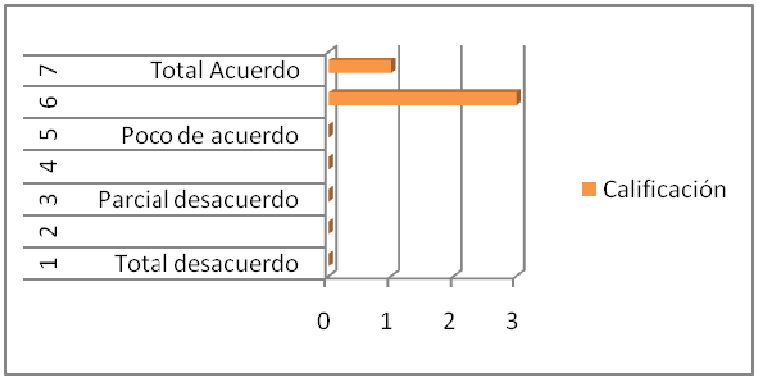
P.15 El comportamiento ético del equipo de LST transmite confianza.

Nivel	Decisión	Calificación
1	Total desacuerdo	0
2	Desacuerdo	0
3	Parcial desacuerdo	0
4	Ni acuerdo, Ni desacuerdo	0
5	Poco de acuerdo	0
6	Casi de acuerdo	1
7	Total Acuerdo	3



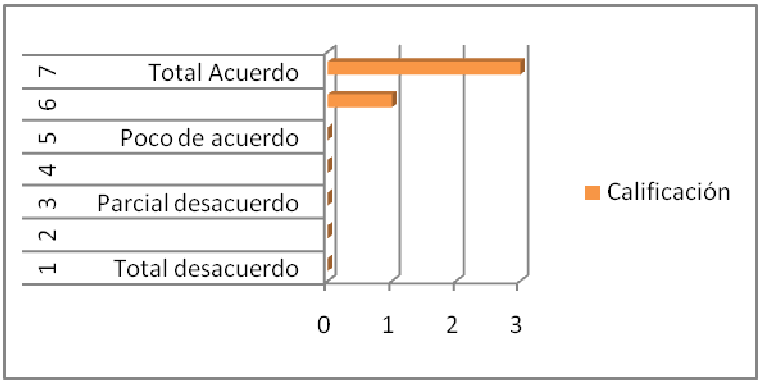
P.16 Usted se siente seguro el momento de ser atendido por LST.

	Decisión	**Calificación**
1	Total desacuerdo	0
2	Desacuerdo	0
3	Parcial desacuerdo	0
4	Ni acuerdo, Ni desacuerdo	0
5	Poco de acuerdo	0
6	Casi de acuerdo	3
7	Total Acuerdo	1



P.17 El equipo de LST es amable con usted

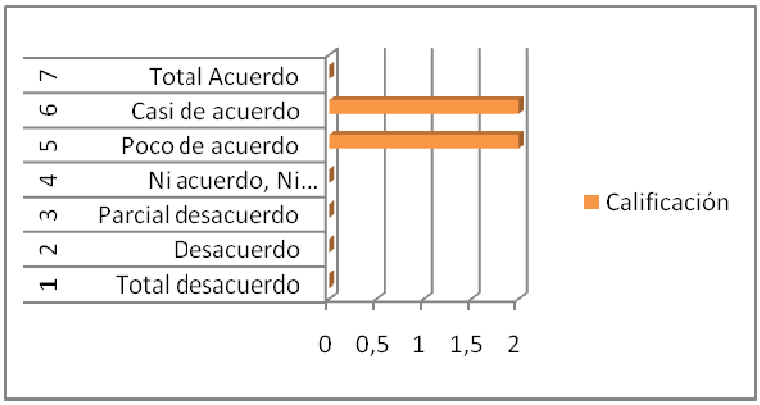
Nivel	**Decisión**	**Calificación**
1	Total desacuerdo	0
2	Desacuerdo	0
3	Parcial desacuerdo	0
4	Ni acuerdo, Ni desacuerdo	0
5	Poco de acuerdo	0
6	Casi de acuerdo	1
7	Total Acuerdo	3



Empatía.- (Atención Individualizada)
P.18 El equipo de LST tiene los conocimientos y destrezas suficientes para proporcionarle una buena atención

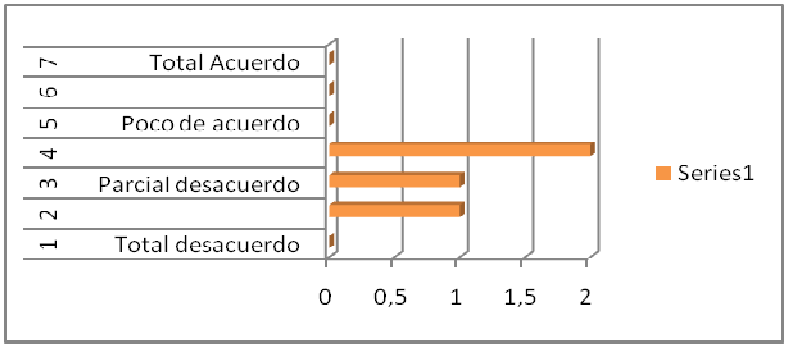
.

Nivel	Decisión	Calificación
1	Total desacuerdo	0
2	Desacuerdo	0
3	Parcial desacuerdo	0
4	Ni acuerdo, Ni desacuerdo	0
5	Poco de acuerdo	2
6	Casi de acuerdo	2
7	Total Acuerdo	0

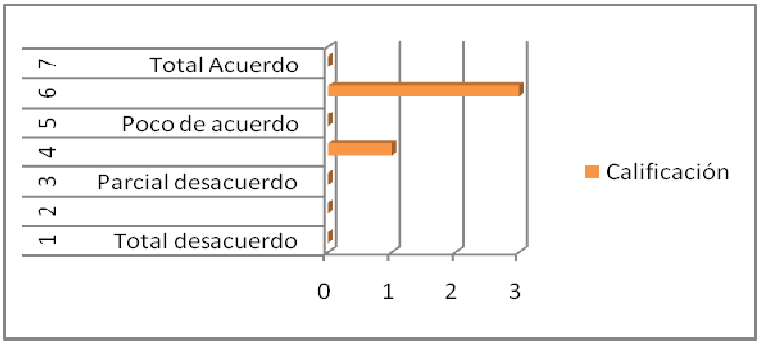


P.19 Los horarios de atención de LST son convenientes a sus intereses.

Nivel	Decisión	Calificación
1	Total desacuerdo	0
2	Desacuerdo	1
3	Parcial desacuerdo	1
4	Ni acuerdo, Ni desacuerdo	2
5	Poco de acuerdo	0
6	Casi de acuerdo	0
7	Total Acuerdo	0

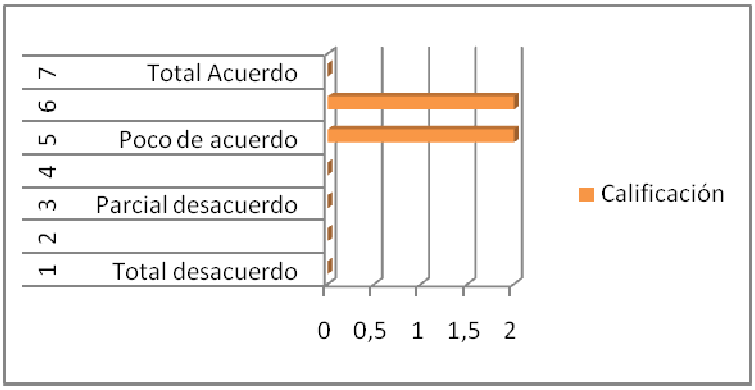


Nivel	Decisión	Calificación
1	Total desacuerdo	0
2	Desacuerdo	0
3	Parcial desacuerdo	0
4	Ni acuerdo, Ni desacuerdo	1
5	Poco de acuerdo	0
6	Casi de acuerdo	3
7	Total Acuerdo	0



P.21 LST entiende las necesidades específicas del cliente

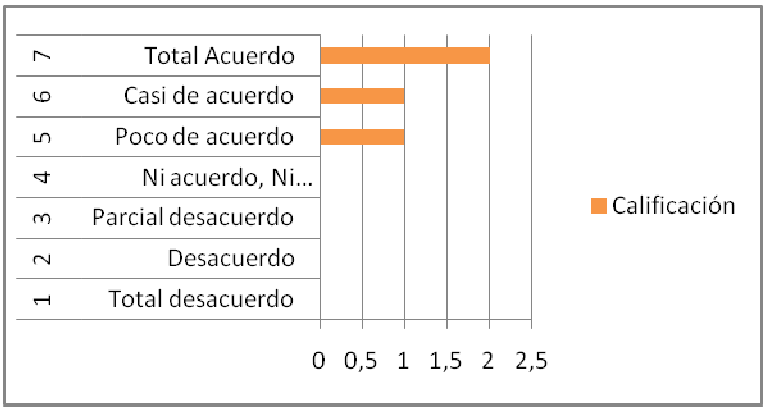
Nivel	Decisión	Calificación
1	Total desacuerdo	0
2	Desacuerdo	0
3	Parcial desacuerdo	0
4	Ni acuerdo, Ni desacuerdo	0
5	Poco de acuerdo	2
6	Casi de acuerdo	2
7	Total Acuerdo	0



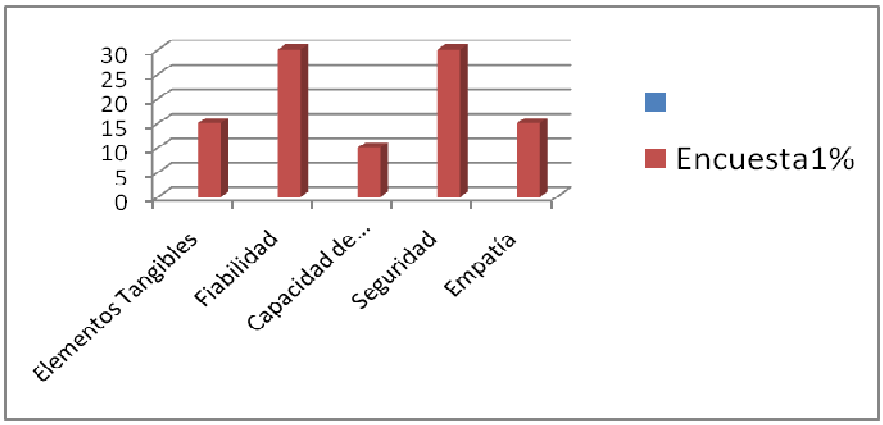
P.22 LST siempre busca el beneficio del cliente.

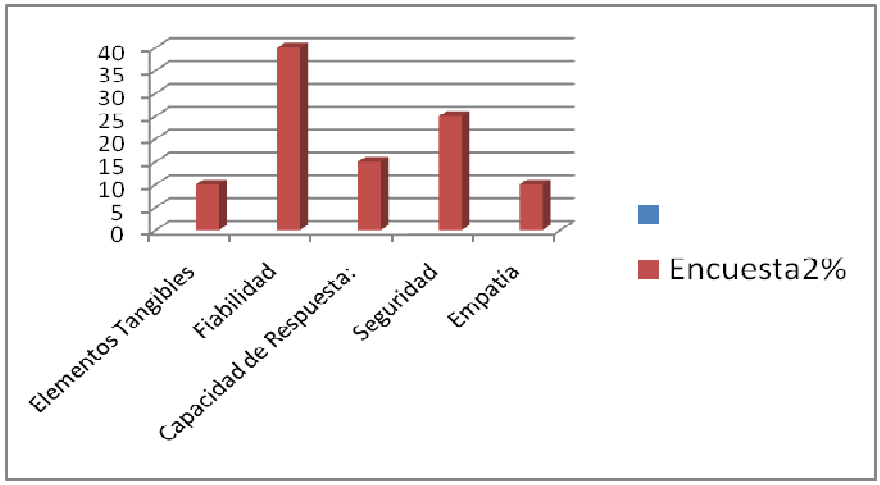
Nivel	Decisión	Calificación
1	Total desacuerdo	0
2	Desacuerdo	0
3	Parcial desacuerdo	0

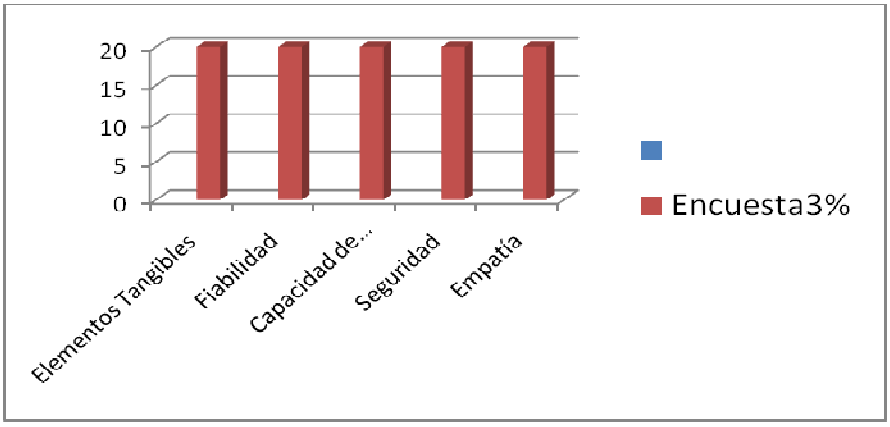
4	Ni acuerdo, Ni desacuerdo	0
5	Poco de acuerdo	1
6	Casi de acuerdo	1
7	Total Acuerdo	2

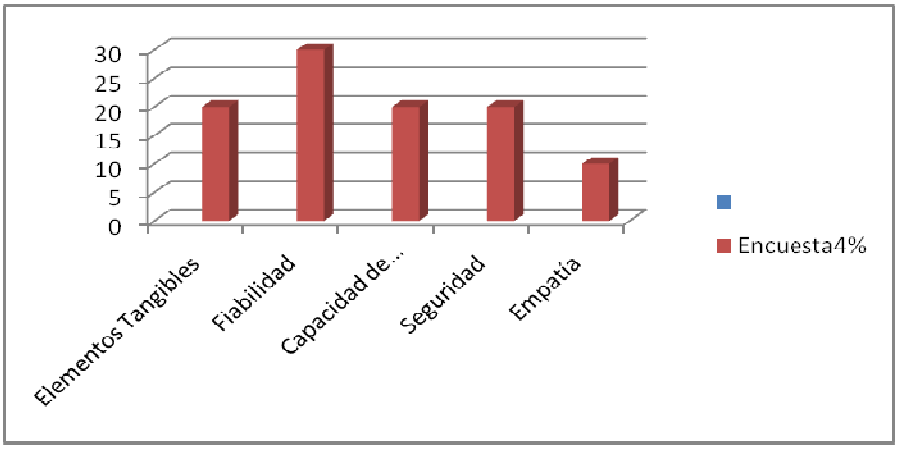


Satisfacción	Encuesta1%	Encuesta2%	Encuesta3%	Encuesta4%
Elementos Tangibles	15	10	20	20
Fiabilidad	30	40	20	30
Capacidad de Respuesta:	10	15	20	20
Seguridad	30	25	20	20
Empatía	15	10	20	10









- **Resultado de las encuestas de la medición del clima laboral:**

1. En relación a las condiciones físicas de su puesto de trabajo (iluminación, temperatura , Ventilación, espacio, volumen de ruidos, etc.) usted considera que este es

Opciones	Resultados
Muy confortable	0
Confortable	0
Poco confortable	4
Incomodo	0
Muy Incomodo	0

2. Usted tiene el suficiente tiempo para realizar su trabajo habitual

Opciones	Resultados
Siempre	1
Casi siempre	1
Algunas veces	2
Casi nunca	0
Nunca	0

3. Está usted de acuerdo en cómo está gestionado el departamento en el que trabaja respecto
a las metas que este tiene encomendadas

Opciones	Resultados
Siempre	0
Casi siempre	4
Algunas veces	0
Casi nunca	0
Nunca	0

4.Considera que recibe, justa retribución económica por las labores desempeñadas

Opciones	Resultados
Siempre	1
Casi siempre	1
Algunas veces	2
Casi nunca	0
Nunca	0

5. Su jefe inmediato tiene una actitud abierta respecto a sus puntos de vista y escucha sus opiniones respecto a cómo llevar a cabo sus funciones

Opciones	Resultados
Siempre	3
Casi siempre	0
Algunas veces	1
Casi nunca	0
Nunca	0

6. Cómo calificaría su nivel de satisfacción por trabajar en la organización

Opciones	Resultados
Muy alto	1
Alto	2
Regular	1
Bajo	0
Muy Bajo	0

7. En mi oficina se fomenta y desarrolla el trabajo en equipo

Opciones	Resultados
Siempre	1
Casi siempre	2

Algunas veces	1
Casi nunca	0
Nunca	0

8. Para el desempeño de mis labores mi ambiente de trabajo es

Opciones	Resultados
Muy malo	0
Malo	0
Regular	3
Bueno	0
Muy Bueno	1

9. Existe comunicación dentro de mi grupo de trabajo

Opciones	Resultados
Siempre	1
Casi siempre	2
Algunas veces	1
Casi nunca	0
Nunca	0

10. Siento que no me alcanza el tiempo para completar mi trabajo

Opciones	Resultados
Siempre	0

Casi siempre	1
Algunas veces	0
Casi nunca	2
Nunca	1

11.Los jefes de la organización se preocupan por mantener elevado el nivel de motivación del personal

Opciones	Resultados
Siempre	1
Casi siempre	3
Algunas veces	0
Casi nunca	0
Nunca	0

12. La relación entre compañeros de trabajo en la organización es

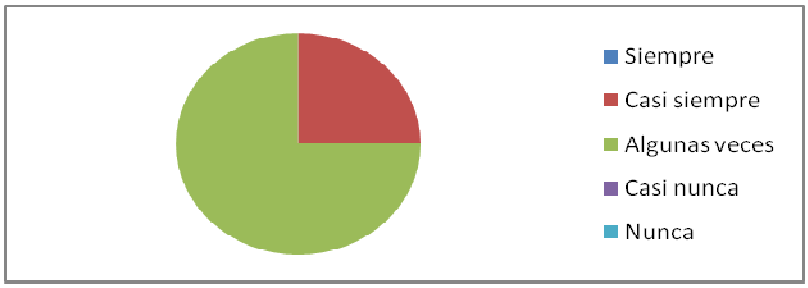
Opciones	Resultados
Muy mala	0
Mala	0
Regular	0
Buena	3
Muy Buena	1

13. La organización otorga buenos y equitativos beneficios a los trabajadores

Opciones	Resultados
Siempre	1
Casi siempre	1
Algunas veces	2
Casi nunca	0
Nunca	0

14. Las remuneraciones están a nivel de los sueldos de mis colegas en el mercado

Opciones	Resultados
Siempre	0
Casi siempre	1
Algunas veces	3
Casi nunca	0
Nunca	0



15. Siento apoyo en mi jefe cuando me encuentro en dificultades

Opciones	Resultados
Siempre	3
Casi siempre	1
Algunas veces	0
Casi nunca	0
Nunca	0

16. Mi jefe me da autonomía para tomar las decisiones necesarias para el cumplimiento de mis responsabilidades

Opciones	Resultados
Siempre	0
Casi siempre	1
Algunas veces	2
Casi nunca	1
Nunca	0

17. Mi jefe me proporciona información suficiente, adecuada para realizar bien mi trabajo

Opciones	Resultados
Siempre	3
Casi siempre	1
Algunas veces	0
Casi nunca	0
Nunca	0

18. El nivel de recursos (materiales, equipos e infraestructura) con los que cuento para realizar bien mi trabajo es

Opciones	Resultados
Muy mala	0
Mala	0
Regular	0
Buena	2
Muy Buena	2
	2

19. Los jefes reconocen y valoran mi trabajo

Opciones	Resultados
Siempre	1
Casi siempre	3
Algunas veces	0
Casi nunca	0
Nunca	0

20. Cómo calificaría su nivel de satisfacción por pertenecer a la organización

Opciones	Resultados
Muy alto	1
Alto	3
Regular	0
Bajo	0
Muy Bajo	0

5.3.9. Anexo 9.

ENCUESTA DE SEGURIDAD INFORMACIÓN

NOMBRE: Eduardo Sierra

CARGO: Gerente

1. ¿Cuántos empleados existen en total en su organización?

   - [x] 1 a 4
   - [ ] 5 a 10
   - [ ] 11 a 20

2. ¿Cuántas personas de tiempo completo o equivalente se dedican a la seguridad informática?

   - [ ] Ninguna
   - [x] 1 a 2
   - [ ] 3 a 5
   - [ ] Más de 5

3. ¿De quién depende la responsabilidad de la seguridad informática de su organización?

   - [ ] Auditoria interna
   - [ ] Director de Seguridad Informática
   - [x] Director Departamento de Sistemas/Tecnología
   - [ ] Gerente Ejecutivo
   - [ ] Gerente de Finanzas
   - [ ] No se tiene especificado formalmente

   Otra:

   ¿Cuál?

4. El cargo en mi organización es:

   - [x] Presidente/Gerente General
   - [ ] Director Ejecutivo
   - [ ] Director/Vicepresidente
   - [ ] Director/Jefe de Seguridad Informática
   - [ ] Profesional del Departamento de Seguridad Informática
   - [ ] Profesional de Departamento de Sistemas/Tecnología
   - [ ] Auditor Interno

   Otra:

   ¿Cuál?

5. El presupuesto global de informática de su organización, incluye aspectos de seguridad de la información?

   - [x] Si
   - [ ] No

6. ¿En qué se centra el gasto de seguridad de su organización? (Elige las que apliquen)

   - [x] Protección de la red
   - [x] Proteger los datos críticos de la organización
   - [x] Proteger la propiedad intelectual
   - [x] Proteger el almacenamiento de datos de clientes
   - [ ] Concientización/formación del usuario final
   - [ ] Comercio/negocios electrónicos
   - [ ] Desarrollo y afinamiento de seguridad de las aplicaciones
   - [ ] Asesores de seguridad informática
   - [ ] Contratación de personal más calificado
   - [ ] Evaluaciones de seguridad internas y externas

Otra:

¿Cuál?

7. ¿Cuál es el presupuesto total previsto para seguridad informática durante el 2010: gastos, hardware, software, asesorías y sueldos? (Elija una. Valores en Dólares)

- ○ Menos de USD$50
- ◉ Entre USD$50 y USD$500
- ○ Entre USD$500 y USD$1000
- ○ Entre USD$1000 y USD$2000
- ○ Entre USD$2000 y USD$5000
- ○ Más de USD$5.000

8. ¿ Durante el año anterior qué casos de violaciones de seguridad tuvieron lugar en su organización? (Elija todas las respuestas aplicables)

- ☐ Ninguno
- ☐ Manipulación de aplicaciones de software
- ☑ Accesos no autorizados al web
- ☐ Fraude
- ☐ Virus
- ☐ Robo de datos
- ☐ Caballos de troya
- ☐ Monitoreo no autorizado del tráfico
- ☐ Negación del servicio
- ☐ Pérdida de integridad
- ☑ Pérdida de información

Otros:

¿Cuáles?

9. ¿Cuántas intrusiones o incidentes de seguridad identificó en promedio durante el año anterior?

- [ ] Ninguna
- [ ] Entre 1-4
- [ ] Entre 4-9
- [x] Más de 10

10. Cómo se enteró de éstas violaciones de seguridad? (Elija todas las aplicables)

- [x] Material o datos alterados
- [x] Análisis de registros de auditoría/sistema de archivos/registros Firewall
- [ ] Sistema de detección de intrusos
- [ ] Alertado por un cliente/proveedor
- [ ] Alertado por un colega
- [ ] Seminarios o conferencias Nacionales e internacionales

Otros:

¿Cuál?

11. Una vez ocurre la violación de seguridad, ésta se notifica: (Elija todas las aplicables)

- [ ] Asesor legal
- [ ] Autoridades locales/regionales
- [ ] Autoridades nacionales
- [ ] Equipo de atención de incidentes
- [ ] Ninguno: No se denuncian

Otro:

¿Cuál? A nuestros A nuestro ISP principal

12. Si se decide no denunciar el incidente de seguridad, ¿cuáles son los motivos o principales preocupaciones? (Elija todas las aplicables)

- ☐ Pérdida de valor de accionistas
- ☐ Publicación de noticias desfavorables en los medios/pérdida de imagen
- ☐ Responsabilidad legal
- ☐ Motivaciones personales
- ☐ Vulnerabilidad ante la competencia

Otro:

¿Cuál?

13. Su organización es consciente de que existe evidencia digital que debe ser identificada, asegurada y analizada, como parte del proceso de atención de incidentes de seguridad informática?

- ◉ Si
- ○ No

14. Durante el año anterior cuántas pruebas de seguridad realizó su organización para valorar el estado de seguridad informática? (Elija una)

- ◉ Una al año
- ○ Entre 2 y 4 al año
- ○ Más de 4 al año
- ○ Ninguna

15. Cuáles de los siguientes mecanismos utiliza actualmente su organización para proteger sus sistemas de información? (Elija todos los aplicables)

- ☐ Smart Cards

- ☐ Biométricos (huella digital, iris, etc)
- ☑ Antivirus
- ☑ Contraseñas
- ☑ Encripción de datos
- ☑ Filtro de paquetes
- ☐ Firewalls Hardware
- ☑ Firewalls Software
- ☐ Firmas digitales/certificados digitales
- ☑ VPN/IPSec
- ☑ Proxies
- ☑ Sistemas de detección de intrusos
- ☑ Monitoreo 7x24

Otros:

¿Cuáles?

16. Usted permanece informado de las fallas de seguridad de sus sistemas a través de: (Elija todas las que aplique)
    - ☑ Notificaciones de proveedores
    - ☑ Notificaciones de colegas
    - ☐ Lectura de artículos en revistas especializadas
    - ☑ Lectura y análisis de listas de seguridad (BUGTRAQ, SEGURINFO, NTBUGTRAQ, etc.)
    - ☐ No se tiene este hábito.
17. Qué describe mejor la política de seguridad de su organización? (Elija una)
    - ◉ No se tienen políticas de seguridad definidas

- [ ] Actualmente se encuentran en desarrollo
- [ ] Política formal, escrita documentada e informada a todo el personal

18. Cuál de los siguientes es el obstáculo principal para lograr una adecuada seguridad informática en su organización?
    - [x] Inexistencia de política de seguridad
    - [ ] Falta de tiempo
    - [ ] Falta de formación técnica
    - [ ] Falta de apoyo directivo
    - [ ] Falta de colaboración entre áreas/departamentos
    - [ ] Complejidad tecnológica
    - [ ] Poco entendimiento de la seguridad informática

19. Su organización (Todo el personal), reconoce la información como un activo más a proteger?
    - [x] Si
    - [ ] No
    - [ ] No Sabe

20. Actualmente la organización posee contactos o relaciones con autoridades nacionales e internacionales para colaborar y recibir asistencia en casos de persecuciones de intrusos?
    - [x] No
    - [ ] No Sabe
    - [ ] Si

    ¿Cuáles?

21. COMENTARIOS

_____Ninguno_____

_____

_____

_____

MUCHAS GRACIAS