UNIVERSIDAD TECNICA DE AMBATO

FACULTAD DE INGENIERIA EN SISTEMAS

TEMA:

"METODOLOGIA PARA LA IMPLEMENTACION DE SISTEMAS SEGUROS DE GESTION DE LA INFORMACION PARA PEQUEÑAS Y MICRO EMPRESAS E INDUSTRIAS"

AUTOR:

MANOLO ROBERTO FABARA VILLACIS

DIRECTOR:

ING. GALO LOPEZ

TESIS DE GRADO PREVIA LA OBTENCION DEL TITULO DE

INGENIERO EN SISTEMAS

AMBATO –ECUADOR

MARZO / 2007

AGRADECIMIENTO

A mi familia por darme el sostén y cariño incondicional que han hecho que crezca como persona tanto espiritual como física e intelectualmente.

A mis padres por darme la vida, darme apoyo y cuidados en todo momento de mi existencia.

A la institución y a todos los que la hacen parte que durante los últimos 7 años me ha visto desarrollarme y crecer y gracias a ellos evolucionar y ser una persona mejor para servir a los demás, gracias a ellos.

A mis hermanas que gracias a que me han indicado el camino no he cometido los errores en ciertas edades.

Al Ing. Galo López por ser la persona que ha guiado de la mejor forma esta tesis.

DEDICATORIA

A mis padres que han sido el sostén en mi vida apoyándome en mis victorias, mis derrotas, mis días malos y buenos, mis penas y alegrías.

A todos mis amigos, compañeros, conocidos, panas, etc. que han pasado por mi vida y que de una u otra forma han sido quienes han forjado lo que soy ahora y espero no defraudarles nunca.

A los que ya no están en este mundo y que con su sabiduría, ejemplo y consejos han hecho que no pierda el camino y siempre quiera ser cada día mejor.

DECLARACION DE AUTENTICIDAD

Yo, Manolo Roberto Fabara Villacís con número de cédula de identidad 1802626570. Declaro que la investigación enmarcada en el diseño de la tesis es absolutamente original, auténtica y personal. En tal virtud, declaro que el contenido, efectos legales y académicos que se desprenden del trabajo de tesis son y serán de mi sola y exclusiva responsabilidad legal y académica.

Manolo Roberto Fabara Villacís

INDICE

INDICE DE FIGURAS Y TABLAS

CAPITULO I GENERALIDADES

1.1. PLANTEAMIENTO DEL PROBLEMA

Desde el advenimiento de la computadora en 1940, cada vez más personas están relacionadas en su trabajo con las mismas, desde analistas, programadores, hasta ejecutivos y directores, en todos los aspectos de la sociedad actual.

Es por esto que en el mundo se genera información electrónica en los variados campos y a los distintos niveles de instituciones y empresas generalmente de forma desordenada y no relacionando los diferentes datos de esta; tomando en cuenta lo anterior podemos entender por que uno de los más altos ejecutivos de IBM expone lo siguiente:

"Frente a la complejidad del mundo, solo sobrevivirán las empresas que hayan aumentado su calidad de información" [1]

Esto nos da una muestra del impacto que ha tenido la tecnología de la información (sistemas de información) en la sociedad y del papel que juega en las empresas e instituciones de todo tipo, por un lado dando ventajas competitivas y por otro ocasionando problemas de toda índole.

Por otra parte en las últimas dos décadas la sociedad en general se ha vista sujeta a vertiginosos cambios, que han afectado directamente al desarrollo de los pueblos específicamente en el ámbito tecnológico.

---

[1] *IBM France (J.-F. David)*

El uso de la Internet además de sistemas de información y redes para el intercambio de datos han influido intrínsicamente si no directamente a dichos cambios lo que ha generado que países desarrollados mejoren la calidad de las servicios que reciben sus ciudadanos con la implementación de sistemas de información de diversa naturaleza que garanticen la equidad de los servicios públicos además de la generación de nuevas clases de servicios que han mejorado su status de vida.

La carencia de sistemas de información y en especial la escasez de sistemas de gestión de la información en países en vías de desarrollo en empresas e instituciones en general ha causado una falta de optimización de recursos y dirección de estos a los departamentos, proyectos, regiones, grupos sociales, provincias, ciudades, etc. que más los necesitan provocando desigualdades sociales, económicas, culturales, etc. que en los últimos años ha causado la falta de competitividad de estas en el mercado, el cierre de otras, el resquebrajamiento de la democracia en varias oportunidades y que muchos ecuatorianos emigren a otros países.

Por otra parte la falta de sistemas integrales de gestión de la información hacen que el usuario o la comunidad en general desconfíe de estas nuevas tecnologías por cuanto en el Ecuador por falta de una verdadera planificación de diversos proyectos causen más problemas en la sociedad que soluciones; ejemplos tenemos a diario como son los servicio que brindan instituciones como el IESS, el SRI, el Registro Civil, etc. y en algo que le afecta directamente en su competitividad a las empresas como son los medios de pago electrónico y los sistemas de información en Internet han hecho que se pierdan muchos negocios empresariales.

Las causas fundamentales para que no existan dichos sistemas son la falta de visión de los beneficios que estos tienen dentro de la sociedad, la falta de recursos económicos y de liderazgo de nuestros dirigentes.

A lo anteriormente planteado se suma la desvinculación entre el Gobierno, Empresas, Colegios Profesionales y Universidades que agudizan el problema es por ello que en vez de que nuestro país de saltos tecnológicos y genere por su propia cuenta tecnología estamos siempre un paso atrás por no decir más de los países desarrollados.

Es por esto que debería ser prioritario para las personas que dirigen al país la realización de sistemas de información que como se mencionó anteriormente mejoren la equidad de los servicios públicos y garanticen una utilización adecuada de los recursos públicos con lo cual tendremos una mejor sociedad en nuestro país el Ecuador.

Ante este panorama tan sombrío la única salida es ir a la cabeza del desarrollo generando nuevas tecnologías o utilizar las últimas tecnologías de los países desarrollados es por esto que mediante la utilización hoy de tecnologías como la de servicios Web, servicios distribuidos, sistemas de manejo de datos más evolucionados (datawarehouse), convergencia de estándares, estándares Internacionales, etc. es como nuestro país y la sociedad en sí va a salir de las crisis que nos afectan en el momento.

1.2 OBJETIVOS

1.2.2 GENERALES

- Realizar una Metodología para la Implementación de Sistemas Seguros de Gestión de la Información para Pequeñas y Micro Empresas e Industrias.

1.2.3 ESPECIFICOS

- Estudio del Sistema de Gestión de la Información para *MYPE*[2].
- Estudio del Sistema de Gestión de Seguridad de la Información.
- Realización de diferentes casos de estudio con el fin de tener una mejor comprensión de lo que conforma un Sistema de Gestión de Seguridad de la Información.
- Crear una metodología para el aseguramiento continuo de la red institucional.
- Proveer la seguridad de redes necesaria para la institución.

1.2.4. JUSTIFICACION

En el Ecuador en este momento vivimos en un tiempo de cambios inmediatos puesto que la globalización y el advenimiento de tratados de libre comercio nos obligan a ello; si no los hacemos vamos a caer en un precipicio del cuál será muy difícil salir.

Uno de estos cambios es en la parte tecnológica y específicamente en la computacional pues es un aspecto tecnológico que no se ha desarrollado en la medida que debiese en nuestro país.

Para realizar estos cambios y llegar a ser competitivos con los demás países debemos dar saltos tecnológicos, ideológicos y jurídicos principalmente puesto que sin la evolución de estos no se podrá tener un país fuerte y a la altura de este nuevo milenio.

[2] *MYPE (Micro y Pequeñas Empresas)*

Nuestro punto de partida debe ser el ya recorrido por países del primer mundo, y es por ello que observando los problemas tanto de seguridad de redes como de privacidad de la información que tienen estos países y el perjuicio que les a ocasionado la falta de políticas y estándares claros que protejan tanto a los ciudadanos como a las micro, pequeñas empresas e industrias y hasta a grandes corporaciones es necesario que países como el nuestro que recién estamos incursionando en el comercio electrónico a toda su capacidad acojan estándares internacionales con lo cual tendremos el mismo o mayor nivel de competitividad que países que hoy se encuentran más adelantados tecnológicamente en América Latina y el mundo que el nuestro.

Pero para que todas estas nuevas tecnologías nos sirvan de provecho y no causen más problemas en vez de solucionarlos debemos realizar verdaderos análisis de las que son necesarias y aplicables de la mejor manera en nuestro país; es decir mediante verdaderos sistemas de gestión de información y sistemas de gestión de seguridad de la información los cuales permitirán tener una visión más clara de lo que realmente necesita primordialmente nuestra organización, empresa o institución para prestar mejores productos y servicios, y como resultado ser más competitiva en el mercado.

Por lo antes planteado se hace necesario realizar un trabajo de investigación que permita plantear una

"METODOLOGIA PARA LA IMPLEMENTACION DE SISTEMAS SEGUROS DE GESTION DE LA INFORMACION PARA PEQUEÑAS Y MICRO EMPRESAS E INDUSTRIAS"

CAPITULO II MARCO TEORICO

2.1 INTRODUCCION

La Micro y Pequeña Empresa e Industria ha sido por excelencia el motor impulsador de economías en vías de desarrollo como la nuestra, pero a que se denomina pequeña o micro empresa o que características posee y las ventajas o desventajas que presenta, etc; razón por la cual es necesario una ambientación al escenario en el que se desarrollará el presente trabajo por lo que inmediatamente se planteará los conceptos básicos de los que nos fundamentaremos en el resto de la tesis.

2.2 CLASIFICACION DE LAS EMPRESAS E INDUSTRIAS

Diversas son las clasificaciones de las empresas pero la más aceptada internacionalmente es la que las identifica según el número de trabajadores que poseen de la siguiente forma:

- Micro 1 - 9 Trabajadores
- Pequeña 10 - 49 Trabajadores
- Mediana 50 - 249 Trabajadores
- Grande 250 y más Trabajadores

2.2.1 MICROEMPRESA

La microempresa está comprendida de personas de limitados ingresos.

Estas iniciativas llamadas microempresas han sido concebidas por emprendedores, quienes se han visto en la desocupación, o con la finalidad de complementar sus

entradas o sencillamente por el ánimo o deseo de aprovechar habilidades y destrezas que poseen.

Por lo antes enunciado podemos determinar que existen microempresas que realizan las más variadas actividades desde un consultorio jurídico o médico hasta el personal que realiza la limpieza o mantenimiento en una casa u oficina.

2.2.1.1 VENTAJAS DE LA MICROEMPRESA

- Al igual que la pequeña y mediana empresa es una fuente generadora de empleos.
- Se transforman con gran facilidad por no poseer una estructura rígida.
- Son flexibles, adaptando sus productos a los cambios del Mercado.

2.2.1.2 DESVENTAJAS DE LA MICROEMPRESA

- Utilizan tecnología ya superada
- Sus integrantes tienen falta de conocimientos y técnicas para una productividad más eficiente.
- Dificultad de acceso a crédito.
- La producción generalmente, va encaminada solamente al Mercado interno.

2.2.2 LA PEQUEÑA EMPRESA

Son parte importante de la economía Mundial. Encontramos en ellas los siguientes tipos:

- Empresas de estilo de vida:

  Estas tienen como intención brindarle a su dueño un estilo de vida confortable.

- Empresas de alto crecimiento:

  Exploran la manera de superar su condición de empresa pequeña lo antes posible. Son conducidas por un equipo de profesionales. Otra de sus intenciones es de lograr amplias utilidades de su inversión.

2.2.2.1 VENTAJAS DE LA PEQUEÑA EMPRESA

- Motiva a los empleados de corporaciones a formar empresas propias, debido a los bajo salaries y sueldos por la agravación que sufre la economía.
- Generación de empleos: Se le atribuye a las pequeñas empresas el mayor porcentaje de generación de empleos de un país. Es por esto que son consideradas como una importante red de seguridad de la sociedad.
- Fomento de la innovación.
- Satisfacción de las necesidades de las grandes compañías: ya que surgen como distribuidoras de las empresas de mayor tamaño, agentes de servicios y proveedores.
- Ofrecimiento de bienes y servicios especializados: Pues las pequeñas empresas resuelven las necesidades especiales de los consumidores.
- Constituye una importante herramienta de la economía de servicios, la cual a ido a través de los años desplazando la economía de escala de las grandes empresas.
- Consta de una técnica de manufactura asistida por computadora: La cual le permite ser tan eficientes como las grandes empresas.
- Poseen organización y estructura simples, lo que le facilita el despacho de mercancía rápido y ofrecer servicios a la medida del cliente.

2.2.2.2 DESVENTAJAS DE LA PEQUEÑA EMPRESA

- Debilidad Tecnológica: al igual que las micro empresas generalmente utilizan tecnología ya superada.
- Debilidad Financiera: por su característica informal; para las instituciones financieras significa un riesgo alto concederles crédito, es por esto que generalmente las pequeñas empresas se ven obligadas a obtener créditos con altos intereses, por montos bajos y a corto tiempo u obtener crédito no formal mediante prestamistas.
- Debilidad Gerencial: la directiva de la empresa no tiene la formación apropiada para liderar la organización.
- Debilidad de Mercadeo/Ventas: especialmente identificada cuando la empresa quiere dar el paso de ser local a regional y aún más cuando desea internacionalizarse.
- Pagan compensaciones en efectivo y prestaciones laborales relativamente bajas.
- La mayoría de empleos generados son de de poco tiempo de duración.
- Sus empleados no cumplen con las reglas de modelo corporativo, por tener un bajo nivel de educación.

2.3 GESTION DEL CONOCIMIENTO

2.3.1 CONOCIMIENTO

Es la facultad para vincular de manera profundamente estructurada, datos e información de un determinado objeto que permiten desenvolverse efectivamente sobre éste en base a un determinado valor y contexto.

2.3.1.1 PRINCIPALES CLASIFICACIONES DEL CONOCIMIENTO

2.3.1.1.1 EL CONOCIMIENTO TACITO

Es aquel que una persona, comunidad, organización o país, tiene integrado o acumulado en su pensamiento, en su cultura y que es complicado de exponer.

2.3.1.1.2 EL CONOCIMIENTO EXPLICITO

Es el conocimiento objetivo y racional que puede ser expresado con palabras, números, fórmulas, etc.

2.3.1.1.3 CONOCIMIENTO INDIVIDUAL

Es el conjunto de saberes de una persona que la llevan a realizar o responder frente a exigencias personales o del contexto.

2.3.1.1.4 CONOCIMIENTO ORGANIZACIONAL

Es la forma en que los recursos de la empresa (o institución) son manejados y convertidos para ejercer una labor productiva que permita la producción de valor.

2.3.1.1.5 CONOCIMIENTO LOCAL

Cuando se entrelaza la cultura con lo local o ecológico brota el llamado conocimiento nativo o local, lo que viene a determinarse como el conocimiento presente y desarrollado en torno a las circunstancias específicas de mujeres y hombres originarios en una zona geográfica concreta.

2.3.1.1.6 CONOCIMIENTO GLOBAL

Se conforma por medio de enlaces sin tener una circunscripción específica, pues quienes lo crean están en varios sitios geográficos. Se elabora a partir de realidades locales, mediante el intercambio de ellas que luego se sistematiza y se abstrae de lo

local.

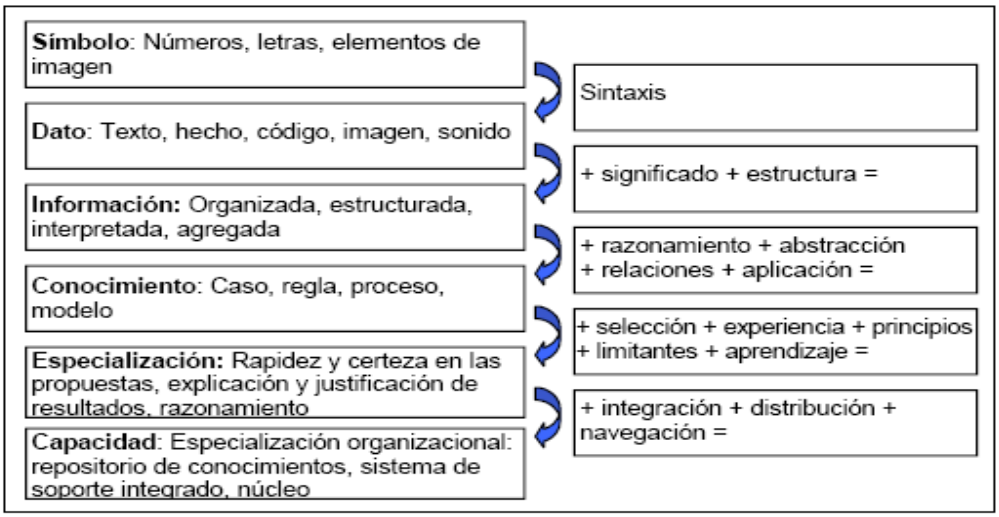


Figura 2.1 La Navegabilidad del Conocimiento [3]

2.3.1.2 ESTRUCTURA DEL CONOCIMIENTO

La estructura del conocimiento	Función del conocimiento	El sistema sobre el cual influyen
VIII. Legitimidad	‣ Aceptación del Proceso	‣ Medio ambiente social Instituciones
VII. Experiencia/Sabiduría	‣ Acción correctiva y de guía	‣ Medio ambiente social
VI. Actividad: (competencia) es igual a "Know-how"	‣ Utilización del conocimiento en el trabajo, en estrategias y políticas	‣ Medio ambiente social
V. Objetivos	‣ Priorización de significados de la comunidad y del hombre, formación de voluntad	‣ Medio ambiente social
IV. Comprensión: Relevancia técnica y moral del conocimiento	‣ Evaluación y conocimiento expresivo y sin palabras El ser humano y la comunidad dan significado o encuentran el significado del conocimiento a mano	‣ Medio ambiente social
III. Conocimiento	‣ Conocimiento como estado consciente Contexto cultural del conocimiento, ej. conocimiento en relación con el medio ambiente Organización social del conocimiento tácito hacia la articulación	‣ Medioambiente psicológico Medio ambiente fisiológico
II. Información	‣ Material en bruto formal y codificado del conocimiento	‣ Medio ambiente técnico Medio ambiente social
I. Datos	‣ Símbolos, caracteres técnicos, reglas de interpretación	‣ Medio ambiente técnico Medio ambiente social
Fenómeno ambiental y natural Herencia cultural, herencia genealógica	‣ Medio ambiente vivo	‣ Medio ambiente físico Medio ambiente natural Medio ambiente cultural

Figura 2.2 Jerarquía del Conocimiento Relacionado a los Objetivos Individuales y su Entorno [4]

[3] *Fuente Beckman , 1997*

2.3.2 CONCEPTO DE GESTION DEL CONOCIMIENTO

Es una disciplina emergente que tiene como propósito engendrar, colaborar y emplear el conocimiento tácito (Know-how) y explícito (formal) existente en un campo definido, para proporcionar respuestas a las necesidades de las personas y de las comunidades en su desarrollo. Esto se ha concentrado en la exigencia actual de manejar el conocimiento organizacional y los aprendizajes organizacionales como herramientas claves para el fortalecimiento de un territorio o espacio en concordancia con las perspectivas de futuro que van a establecer sus objetivos estratégicos de desarrollo en el mediano y largo plazo.

No se debe olvidar que estamos gestionando personas, cultura y tecnologías.

2.3.3 EL CICLO DE LA GESTION DEL CONOCIMIENTO

Se ha determinado seis fases o etapas en el ciclo permanente que permiten incorporar como práctica habitual la gestión de conocimiento en una institución que maneja el conocimiento organizacional como su recurso estratégico más precioso. **Figura 2.3**

2.3.3.1 ETAPA 1: DIAGNOSTICO INICIAL DE LA GESTION DEL CONOCIMIENTO

Definir la situación en que se halla el sistema de Gestión de Conocimiento al interior de la institución, con lo cual se van a determinar las necesidades de esta. Para ello se utilizarán las siguientes técnicas:

---

[4] *Fuente : Ministerio de Trabajo de Finlandia, Helsinki, 2000*

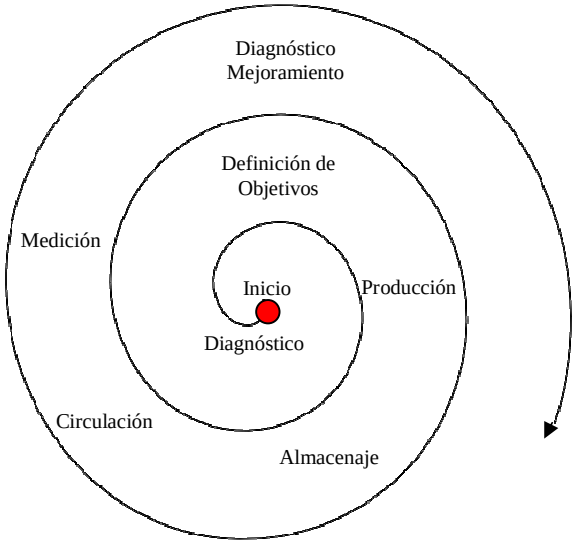


Figura 2.3 Ciclo de la Gestión de Conocimiento

2.3.3.1.1 MAPA DE CONOCIMIENTO ORGANIZACIONAL

Desde el punto de vista del diagnóstico, la pregunta que interesa responder en relación con el conocimiento organizacional es la siguiente: ¿Cuánto sabe de lo que sabe? Utilizando la metodología adecuada, se configura un diagrama que permite identificar:

a) Lo que sabe que sabe: El conocimiento que la organización sabe que conoce

Se relaciona con lo que está o podría estar siendo aplicado eficazmente para solucionar problemas.

b) Lo que sabe que no sabe: El conocimiento que la organización requiere pero que sabe que no posee.

Puede ser formado, examinando las competencias requeridas y manejando los programas de enseñanza convenientes.

c) Lo que no sabe que sabe: El conocimiento que la organización posee y que no está siendo utilizado.

Las prácticas de gestión del conocimiento concernientes con la identificación, captura, almacenamiento y transmisión facultan que este recurso pueda ser empleado y explotado por todos.

d) Lo que no sabe que no sabe: El conocimiento que la organización ignora que no conoce (pérdida o carencia no visualizada).

Requiere de un estudio más completo para revelar aquel conocimiento que se carece o que se ha perdido, lo que posibilita detallar las tácticas para su reposición o incorporación en la dimensión que continúe siendo clave para el ejecución de los objetivos de la institución.

2.3.3.1.2 DIAGNOSTICO DE PRACTICAS HABITUALES

Las necesidades que se obtienen del análisis de los flujos de conocimientos pueden definirse según su nivel de utilidad, desde conocimiento sin valor hasta conocimiento estratégico, con una variedad de grados intermedios dependiendo de la profundidad que se quiera lograr con el diagnóstico.

2.3.3.1.3 ALINEACION DE NECESIDADES EN RELACION A LAS FUENTES DE CONOCIMIENTO

a) Conocimiento Estratégico, imprescindible o muy útil cuya fuente existe y se puede utilizar" Grado óptimo de alineación".

b) Conocimiento Estratégico, imprescindible o muy útil cuya fuente no existe. Recurso que falta. Requiere adquisición.

Si las fuentes y las necesidades no están mayoritariamente alineadas, el esfuerzo de la Gestión de Conocimiento estará concentrado en adquirir el conocimiento faltante, ya

sea vía la producción interna o por medio de los proveedores externos de conocimiento experto.

c) Conocimiento sin valor, inútil o escasamente útil cuya fuente existe Recurso Obsoleto. Requiere actualización, modificación, depuración, reconversión o eliminación, transformar el conocimiento obsoleto en conocimiento actualizado.

La combinación entre el Diagnóstico de Prácticas Habituales y el Mapa de Conocimiento Organizacional, da como resultado los tipos de conocimientos que se movilizan entre proveedor y destinatario.

2.3.3.1.4 EVALUACION DE LAS CAPACIDADES DINAMICAS DE LA ORGANIZACION

El diagnóstico basado en las capacidades dinámicas pretende, en definitiva, evaluar la calidad del aprendizaje organizacional, midiendo el comportamiento de los sistemas de gestión del conocimiento ya operativos.

La evaluación se realiza tanto a nivel individual como colectivo. La capacidad de absorción individual examina los comportamientos relacionados al aprendizaje proactivo, en tanto que la capacidad de absorción organizacional se evalúa de acuerdo a la existencia de políticas o procedimientos formales o informales que fomentan dicho aprendizaje. Los efectos de la capacidad de absorción se miden tanto en los procesos de adquisición de información y know-how, como también en el proceso de creación de conocimiento nuevo y necesario para entregar las respuestas que el medio ambiente está demandando.

2.3.3.2 ETAPA 2: DEFINICION DE LOS OBJETIVOS DEL CONOCIMIENTO

Se definen como objetivos de conocimiento a aquellos que proporcionan una dirección a la Gestión de Conocimiento en relación con la creación de conocimientos y de competencias claves para fortalecer el desarrollo de sus estrategias.

En la práctica, los proyectos de Gestión de Conocimiento se van realizando por fases concatenadas en las cuales se intenta lograr algunos de los propósitos globales relacionados a esta doctrina, lo que faculta ir adaptando los pasos subsiguientes a la cultura preponderante en el medio sobre el cual se aplica.

Se ha establecido tres tipos de objetivos de conocimientos:

a) Objetivos de conocimiento normativo, están encaminados a la toma de conciencia del valor del conocimiento por parte de la institución.

b) Objetivos estratégicos del conocimiento, que determinan el conocimiento clave para la institución y las exigencias de conocimiento nuevo.

c) Objetivos de conocimiento operativo, los cuales se refieren con la implementación de la gerencia del conocimiento, cambiando los dos anteriores en metas concretas.

El diagnóstico inicial dirige las iniciativas y añade una posibilidad de factibilidad a los propósitos y expectativas que se han expuesto con la visión.

2.3.3.3 ETAPA 3: PRODUCCION DE CONOCIMIENTO ORGANIZACIONAL

Se ha definido dos modelos de creación de conocimiento organizacional que corresponden a:

2.3.3.3.1 MODELO OCCIDENTAL DE GENERACION DE CONOCIMIENTO ORGANIZACIONAL

El Modelo Occidental se elabora sobre la concepción de que la elaboración y aprendizaje de conocimiento nuevo tiene su origen en las Preguntas, Cuestionamientos, Problemas o Necesidades de las personas, grupos u organizaciones, las cuales dan ocasión a una serie de concepciones en la investigación de las respuestas apropiadas. Estas ideas se sujetan a prueba y mediante el razonamiento se reconocen las mejores soluciones, que son el conocimiento nuevo.

Según las contribuciones efectuadas por algunos autores, este modelo se relaciona con la tendencia de cambiar los enfoques conductistas anteriores por un modelo constructivista en la construcción de ambientes. El Modelo Constructivista, concibe al proceso de construcción de conocimiento ecológico o de contexto, como un sistema formado por diversos actores: las personas que aprenden y construyen, las instituciones, la cultura, el ecosistema, etc. señalando a cada uno el papel que le corresponde dentro de este contexto integrado encaminado a solventar las exigencias de aprendizaje. Este modelo está basado en los siguientes principios del aprendizaje:

Figura 2.4

2.3.3.3.2 MODELO ORIENTAL DE GENERACION DE CONOCIMIENTO ORGANIZACIONAL

Así como el modelo occidental está basado en la capacidad intelectual de las organizaciones, el fundamento del Modelo Oriental está en las experiencias de los sujetos que conforman dichas organizaciones. Dado que estas experiencias provienen de conocimientos tácitos, el método de creación de conocimiento organizacional

oriental busca la transformación del conocimiento tácito individual en conocimiento explícito colectivo.

Existen cuatro formas de conversión de conocimiento, las que constituyen el motor del proceso de creación de conocimiento por medio de las etapas: Socialización, Externalización, Combinación e Internalización **Figura 2.5**

1. Aprendemos con dos hemisferios cerebrales.	Izquierdo: Lógico, sistémico, analítico, objetivo, estructurado. Derecho: Intuitivo, subjetivo, espontáneo, flexible, sintético.
2. Cada persona utiliza diferentes estilos de aprendizaje.	Aprendizaje Dinámico, Creativo, Analítico, Pragmático [McCarthy, 1997]
3. Existen diferentes tipos de inteligencias: Inteligencias Múltiples.	Lógico/matemático, Interpersonal, Intrapersonal, Musical, Quinético, Visual, Verbal [Gardner, 1995]
4. Nuestro pensamiento es radial asociativo.	La mente memoriza por partes y aprende por totalidades. Para integrar datos la mente utiliza el enfoque radial. [Buzan,1993]
5. Aprendemos a través de las sensaciones.	Captamos el mundo a través de los órganos sensoriales o sistemas representativos.
6. Aprendemos lo que necesitamos saber para satisfacer una necesidad.	Sólo percibimos (aprendemos) lo que nos interesa. Sólo nos interesa (aprendemos) lo que necesitamos. Aprendizaje significativo.
7. Aprendemos cuando participamos en la construcción de los conocimientos.	La experiencia de muchas personas dice que cuando un ser humano construye, inventa o diseña algo, este algo se convierte en parte de su vida y difícilmente lo olvidará.
8. El aprendizaje es mayor cuando compartimos experiencias y conocimientos.	Ninguna persona es poseedora de la verdad absoluta. Cada cual tiene parte de la verdad. La única forma de aumentar nuestra riqueza cognoscitiva es combinar las distintas verdades de las distintas personas.
9. Aprender es el proceso de descubrir lo que sabes pero no sabes que sabes.	Educar viene del latín "educere": sacar y desarrollar lo que está adentro. Dimensión tácita del conocimiento.
10. Aprendes lo que crees que puedes aprender.	Fenómeno de la profecía auto-cumplida (Efecto Pigmalión)
11. Facilitar el aprendizaje para el futuro	Por medio de: Aprender a hacer, aprender a ser, aprender a aprender y aprender a convivir.

Figura 2.4 Principios de Aprendizaje Significativo[5]

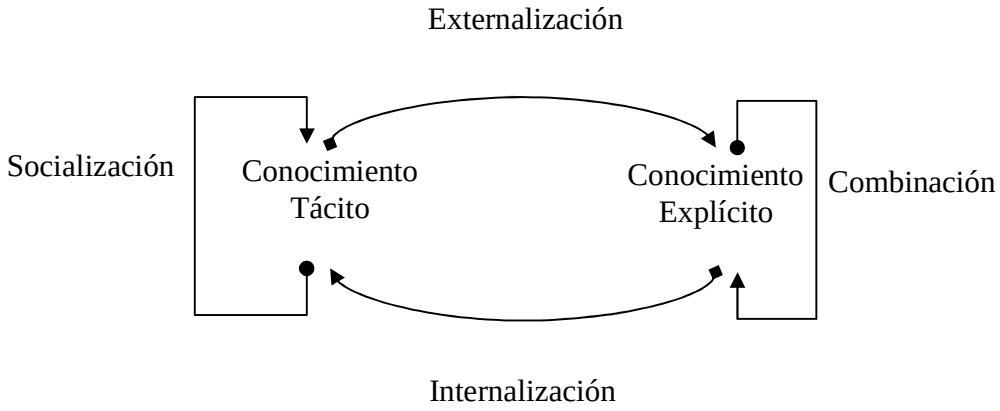


Figura 2.5 Transformación del Conocimiento

[5] *Fuente : Adaptación desde Brenson, Gilbert; "Constructivismo Criollo"*

En cada una de las etapas, se producen los efectos que se indican en el siguiente cuadro resumen:

MODELO ORIENTAL DE GENERACIÓN DE CONOCIMIENTO

Etapa del Ciclo	Tipo de Conversión	Descripción	¿Cómo se logra?	¿Qué resultado genera?
Socialización (SINTONIZAR)	‣ Tácito a tácito	‣ Compartir y crear conocimiento tácito a partir de las experiencias	‣ Caminando y conversando ‣ Observando ‣ Transfiriendo experiencias	‣ Conocimiento armonizado o compartido
Externalización (GENERAR)	‣ Tácito a explicito	‣ Articular conocimiento tácito a través del diálogo y la reflexión	‣ Expresar por medio del Lenguaje Común ‣ .Traducir a conceptos, analogías, metáforas, mapas y modelos	‣ Conocimiento conceptual
Combinación (COMPARTIR)	‣ Explicito a explicito	‣ Sistematización de conceptos con el conocimiento ya almacenado y la información disponible por medio de operaciones mentales colectivas	‣ Acumular e integrar conocimiento explícito ‣ Transferir y difundir ‣ Editar y publicar conocimiento explícito	‣ Conocimiento Sistémico
Internalización (UTILIZAR)	‣ Explicito a tácito	‣ Aprender y adquirir nuevo conocimiento tácito a partir de la práctica (aprender haciendo)	‣ Aprender conocimiento explícito haciendo o produciendo.	‣ Conocimiento Operativo

Figura 2.6 Modelo Oriental de Generación de Conocimiento[6]

Es preciso precisar que en este proceso se originan ineludiblemente errores como fallas en la transmisión de las ideas en su conjunto, obstáculos comunicacionales, interpretaciones con relaciones erradas, etc.

El rol de la dirección en el proceso de construcción de conocimiento es el de proporcionar el contexto adecuado para facilitar las tareas grupales y la elaboración y aglomeración de conocimiento tanto al nivel individual como organizacional.

2.3.3.4 ETAPA 4: ALMACENAJE Y ACTUALIZACION

Esta fase se caracteriza por la acumulación de los conocimientos preliminarmente codificados, situándolos en repositorios desde los cuales los usuarios pueden acceder fácilmente, adecuadamente y en el momento que se necesite al conocimiento.

[6] *Fuente : Adaptación de Nonaka, Konno*

La fase de Almacenaje y Actualización de conocimientos, requiere la realización coordinada y sistemática de las siguientes labores: Codificación, Catalogación, Depuración y limpieza y Seguridad.

2.3.3.4.1 CODIFICACION DE CONOCIMIENTOS

La codificación es la representación del conocimiento tácito o explícito de manera que pueda ser accesado y compartido, y concierne al enlace entre la etapa de Elaboración y la etapa de Almacenaje cuando el creador ha resuelto participar lo que sabe o lo que ha creado. La manera de representación tiene que ver con el uso del lenguaje más adecuado al sistema-entorno que se empleará el conocimiento codificado con algún objetivo posterior. La consecuencia de este proceso se llama en forma usual *CONTENIDO*.

Tradicionalmente los Contenidos se sitúan en *CONTENEDORES*, que son repositorios o estructuras específicas según los tipos y formatos en que se hallan codificados tales contenidos. La práctica de lenguajes y el uso de Diccionarios permiten desarrollar un proceso de codificación de calidad, como también el uso de ciertas herramientas tecnológicas que asisten a elaborar contenidos sobre la base de símbolos que constituyen objetos de la realidad, los cuales se integran para representar ideas de manera abreviada y visual. La agrupación de Contenedores constituye lo que se designa la Memoria Organizacional.

En el siguiente cuadro se describen los tipos de depósitos o contenedores de conocimientos y los objetos que permiten almacenar:

Tipo de Contenedor	Descripción	Contenido
Bancos de Conocimientos	Almacenan amplias cantidades de conocimientos en forma de documentos, Formularios, Informes, Gráficos, mapas u otros	Bancos de ideas Bancos de Historias Mejores Prácticas Lecciones Aprendidas Mapas de Conocimientos
Bancos de Competencias	Almacenan contenidos relacionados con las competencias de las personas	Páginas Amarillas Arboles de Competencia Conocimiento de expertos Mapas de Competencias
Sistemas de Bibliotecas	Permiten almacenar meta datos relacionados con el contenido físico de bibliotecas	Meta descriptores de libros, revistas, informes, papers y otros
Diccionarios (Thesaurus)	Permiten almacenar diccionarios virtuales (palabras, descriptores, significados)	Diccionario de competencias Diccionario organizacional Lenguaje de usuarios Lenguajes locales o ecológicos
Bodegas de datos (DataWarehouses)	Contienen grandes volúmenes de datos estructurados, los cuales pueden ser accesados a través distintas tecnologías (DataMining)	Bases de datos organizacionales
Bancos de Proyectos	Almacenan datos, información y conocimiento sobre proyectos realizados, en curso o finalizados.	Documentación de manejo de proyectos
Bancos de mensajes	Administran la correspondencia electrónica que circula a través de la organización	Correos electrónicos
Contenedores múltiples	Almacenan contenidos de diversos tipos, formatos y métodos de acceso.	Knowledge Center Information Center

Figura 2.7 Contenedores y Contenido [7]

2.3.3.4.2 CATALOGACION DE LOS CONTENIDOS

Los contenidos codificados deben ser apropiadamente ordenados por expertos que están capacitados para comprender el sentido y significado de los variados elementos fuente y, por otra parte, detallar y solucionar el lugar, descriptores, meta-datos y manera definida en que se originará el almacenamiento, en correlación con ciertos principios estándares especificados para tales fines.

[7] *Fuente : Peluffo A. y Catalán C. ILPES 2002*

2.3.3.4.3 DEPURACION Y LIMPIEZA DE CONTENIDOS

Constituye, sin lugar a dudas, la única elección para que el conocimiento codificado, ya sea tácito o explícito, no disminuya su validez y sirva a los objetivos de todos los integrantes de la institución en el instante en que éstos lo demanden. De la misma manera, la adecuada depuración de contenidos proporciona la liberación de espacio que origina una mayor eficiencia en los procesos de actualización de contenidos y mejores tiempos de respuesta frente a requerimientos de los usuarios.

2.3.3.4.4 SEGURIDAD DE LOS CONTENIDOS

Una las funciones más relevantes de los encargados de los Bancos de Conocimiento es proporcionar todos los elementos de seguridad necesarios para evitar que los contenidos sean dañados, casual o intencionadamente. Para esto, deben contar con las facilidades que les permitan establecer controles de acceso, filtros u otros procedimientos que puedan resultar poco amistosos en el contexto de una comunidad de usuarios.

2.3.3.5 ETAPA 5: CIRCULACION Y UTILIZACION DE CONOCIMIENTOS DE LOS USUARIOS

En conjunto con los espacios de aprendizaje, estos ambientes son los propicios para que los conocimientos puedan fluir de manera ininterrumpida, de manera que se logre el objetivo de la distribución y el uso de tal conocimiento.

Los usuarios pueden cooperar de una manera pasiva o activa, sin embargo se fomenta la interacción para afinar los servicios que se prestan. En ambientes de participación más activos, se generan redes de colaboración comunitaria que tienden a dar respuestas más rápidas a los problemas comunes.

2.3.3.6 ETAPA 6: MEDICION DEL DESEMPEÑO

Esta es una fase que está presente periódicamente y su propósito es establecer en cada uno de los ciclos en que se realiza la medición misma, la tendencia en los indicadores que se han escogido para visualizar de qué forma la Gestión de Conocimiento está provocando impactos en los efectos esperados en la institución, sea esta del ámbito privado o público.

En este sentido, los indicadores permitirán conocer:

a) ¿Qué capacidad de generación de conocimiento ha desarrollado la institución a partir de el establecimiento de las prácticas de Gestión de Conocimiento?

b) ¿Cómo se están compartiendo los conocimientos tácitos y explícitos existentes?

c) ¿Cuál es la tasa de utilización del conocimiento que está disponible en la organización?.

Alrededor de estas preguntas se construyen los indicadores específicos que aplicarán en cada caso particular.

En la mayor parte de los casos de proyectos asociados a la medición del capital intelectual, los participantes comienzan definiendo los indicadores que se usarán en la medición y los criterios de desempeño esperados para estos indicadores. Posteriormente, se determina la fuente de información a partir de la cual se obtendrá la retroalimentación necesaria para los procesos de medición y en último caso, se define y construyen las herramientas tecnológicas que apoyarán cada etapa.

2.4 INTRODUCCION A LA SEGURIDAD DE LA INFORMACION

2.4.1 LA INFORMACION EL RECURSO QUE SE DEBE PROTEGER

En las empresas e instituciones generalmente se tiene salvaguardas para los diferentes recursos de esta, especialmente los activos de la misma pero nunca han reflexionado que la información como tal puede ser mucho más importante, puesto que facilita el diario desarrollo y el mejoramiento de estas siendo la razón en algunos casos de el por que del éxito de estas organizaciones es por esto que debemos salvaguardar la información, el conocimiento y el tránsito de este en nuestra institución o fuera de ella a lo cual la ISO[8] 17799 dice lo siguiente:

"La información es un recurso que, como el resto de los importantes activos comerciales, tiene valor para una organización y por consiguiente debe de ser debidamente protegida."

La seguridad de la información protege de una amplia gama de amenazas, a más de garantizar la continuidad comercial, minimizar el daño al mismo y maximizar el retomo sobre las inversiones y las oportunidades." (ISO-lEC 17799 - Año 2000)

"Cualquiera sea la forma que adquiere la información, o los medios por los cuales se distribuye o almacena, siempre debe ser protegida de forma adecuada" (ISO-IEC-17799)

Pero para la correcta apreciación de lo que debemos proteger debemos clasificar de alguna forma la información para lo cuál la ISO 17799 lo ha realizado de la siguiente forma por categorías:

- Activos de información (datos, manuales de usuario, etc...)

[8] ISO siglas en Ingles de la International Standard Organization

- Documentos de papel (contratos)
- Activos de software (aplicación, software de sistemas, etc...)
- Activos físicos (computadoras, medios magnéticos, etc...)
- Personal (clientes, personal)
- Imagen de la compañía y reputación
- Servicios (comunicaciones, etc...)

2.4.2 CONCEPTO DE SEGURIDAD DE LA INFORMACION

Antes de presentar un concepto de lo que es seguridad el cual lo aplicaremos en el resto de la tesis pretendemos determinar el que comúnmente se tiene respecto de este término y lo haremos presentando su definición en el diccionario:

Seguridad:

(sustantivo femenino). Certeza, firmeza, confianza.

Sin riesgo (sust.) Dicese de las cosas ciertas, firmes y/o libres de peligro o riesgo. Estado de las cosas bajo protección (lat. Securitis) Confianza, tranquilidad de una persona procedente de la idea de que no hay ningún peligro que temer

Como veremos más adelante el concepto de seguridad ha evolucionado de diferentes formas durante la historia y de acuerdo a las diferentes culturas que lo han tratado de formular puesto que es muy ambiguo es por ello que manejaremos el concepto proporcionado por el estándar IS017799 que es el que lo usaremos en todo el desarrollo de la tesis.

La seguridad de la información se define como la preservación de las siguientes funcionalidades:

- Integridad

- Confidencialidad
- Disponibilidad

Tanto de los recursos como de la información

Pero a que nos referimos con estos tres términos, comencemos con la integridad y tomemos el ejemplo del Juego de niños "El teléfono Roto" en el cual el objetivo del Juego era el de pasar un mensaje de niño a niño sin que supieran el resto hasta que le llegara el tumo de escucharlo por el oído; al terminar la hilera de niños se decía el mensaje en voz alta el cual generalmente era totalmente diferente que con el que se comenzaba en el otro extremo de la hilera si esto sucede en una empresa o en un sistema informático tendríamos que durante la transmisión de los datos desde el punto que se generaron hasta el punto donde se guardan estos hubo un error y en el caso de un banco en una cuenta determinada un depositante en vez de tener 10 dólares ahora tiene 100 o al contrario o en caso de un sistema en el cual se automatiza los datos personales de los usuarios (sean estos empleados o clientes) de una institución se tendrá que en vez de sexo masculino se tendrá sexo femenino o al contrario, esto pudiera haber sido ocasionado por el cambio de datos en el origen destino o durante la comunicación por la intromisión de un agente externo sea este un hacker, un virus, etc. A esto consideramos como integridad el combate a que los datos sean corrompidos.

En el caso de la confidencialidad según nuevas leyes y reglamentos tanto de países desarrollados como en los en vías en desarrollo se ha observado que este aspecto es muy determinante en lo que se refiere a seguridad puesto que se ha establecido que la información es un arma estratégica la cual la deben tener solo personas autorizadas y

que en una compañía o institución puede determinar su éxito o fracaso en el mundo comercial y globalizado; es por esto que desde que se genera la información es decir desde el remitente hasta el destinatario debe de ser protegida con los permisos y encriptación pertinentes para que solo la persona indicada o autorizada pueda receptarla y así un competidor, espía industrial o hacker no pueda descifrarla.

Al igual que las anteriores la disponibilidad de la información es muy importante en algunos tipos de sistemas de información más que en otros puesto que pueden ser este aspecto de vida o muerte principalmente en sistemas de alto riesgo como son sistemas médicos o de tiempo real pero también este concepto puede causar la quiebra o repunte de una empresa; tomemos como ejemplo si una empresa no tuviera luz los empleados no podrían hacer funcionar las máquinas con lo cual se generaría un perjuicio incalculable, lo mismo sucede en una proveedor de espacio para sitios web puesto que si su servidor cae sea por un ataque de denegación de servicio o por la intrusión de un hacker y tiene que parar de dar su servicio, cientos o miles de negocios no podrán vender sus productos por internet o contactarse con sus proveedores o tan solo promocionar sus productos y servicios con lo cual perderán clientes y esto les podría llevar a la bancarrota. Pero si al contrario este proveedor de espacios para páginas web presta un servicio que es altamente confiable va a aumentar el número de clientes y ganar una posición en el mercado y un prestigio en el ámbito en que se desenvuelve y este valor agregado también es transmitido a sus clientes los cuales pueden decir con certeza que se pueden comunicar con ellos los 365 días del año 7 días a la semana 24 horas al día si es el caso.

2.4.3 HISTORIA Y EVOLUCION DE LA SEGURIDAD

2.4.3.1 HISTORIA

Los conceptos primitivos de seguridad como son de alertar, evitar, detectar, alarmar y reaccionar son tan viejos como la humanidad misma, siendo una parte esencial de la disputa diaria por la vida, y están fundados en el instinto básico de conservación es por esto que no es coincidencia que algunos de los más complejos controles de protección imiten de alguna manera estas ideas fundamentales.

Pero más tarde que temprano los seres humanos aprendieron vertiginosamente que la mera existencia de medidas protectoras era frecuentemente suficiente para descorazonar a los adversarios con intenciones agresivas. Dolorosas experiencias enseñaron a los atacantes que buscaban penetrar las organizadas defensas que las pérdidas eran a menudo inaceptables y frecuentemente fueron disuadidos de nuevos ataques.

Los conceptos de seguridad siguieron evolucionando con los aportes de varias culturas, el aumento de la conciencia del hombre respecto de lo que quería proteger y que era lo más prioritario para el. Luego en los diferentes tipos de gobierno desde la tiranía, oligarquía, dictadura y democracia aparecieron conceptos diferenciados entre la seguridad pública y privada donde la primera se dedicaba a la protección general de la población tanto externa como internamente de una nación, imperio, reino, etc. y la segunda era privilegio de personajes importantes de la sociedad por lo cual se comenzaron a gestar grupos dedicados enteramente a esta ocupación con entrenamientos especializados tanto físicamente como en la parte intelectual. Así comenzaron a aparecer grupos que evolucionaron progresivamente hasta lo que hoy

conocemos como son en el aspecto público las fuerzas armadas, policía, grupos especializados, etc. y en el aspecto privado grupos de seguridad privada de toda índole.

En estos tiempos la seguridad pública es una preocupación importante para cualquier gobierno. Actividades y sistemas de seguridad son operados en muchas organizaciones, desde agencias gubernamentales y plantas industriales hasta hospitales, iglesias y colegios que son clasificados o diferenciados como sistemas de seguridad informática, industrial, física, ocupacional, etc.

Ahora de acuerdo a la era en la que se ha encontrado la humanidad ha desarrollado seguridades para proteger el bien más preciado que ha identificado generalmente a dicho periodo de tiempo de la humanidad y en el caso del tiempo en que vivimos es llamada la era de la comunicación, la información y el conocimiento por lo cual se han ingeniado sistemas y productos de diversa índole con el afán de proteger todos estos recursos.

2.4.3.2 EVOLUCION

Evolución de las seguridades en los últimos 40 años 1965 Departamento de defensa de los Estados Unidos

- 1983 Encriptación de la información
- 1985 virus y Antivirus
- 1990 Seguridad en redes
- 1995 Firewalls
- 2000 Seguridad en sistemas operativos IDS's
- 2003 Seguridad Informática Global

La seguridad es hoy en día una profesión compleja de funciones especializadas.

Nuevos sistemas de comunicación, biométricos, de detección y tecnologías informáticas han añadido nuevas herramientas al arsenal de la seguridad, que hasta los tiempos recientes estaba basado (como en la era de los Faraones) en armas, trampas, cerraduras, cajas fuertes, puertas blindadas y barrotes. Todos estos nuevos instrumentos que la ingenuidad humana ha concebido (cajas fuertes y cerraduras "electrónicas", sistemas de alarma computerizados y centralizados, circuitos cerrados de televisión, equipos de contra-vigilancia, etc...) son ahora los nuevos ingredientes de los programas de seguridad. Los sistemas de seguridad son cada vez más automáticos, particularmente aquellos de detección y comunicación de siniestros, y en una extensión menor, aquellos relacionados con la valoración, la decisión y la reacción. Los avances en la miniaturización se reflejan en los equipos de seguridad que cada vez son más pequeños, más baratos, más fácilmente instalados y mantenidos, y más confiables. Pero todavía, debería ser reconocido que la tecnología, aunque importante y coherente con la aplicación de los principios de la seguridad, no ha añadido ningún nuevo concepto a aquellos ya conocidos anteriormente. Por el contrario, parece que ha abierto nuevas vulnerabilidades y a aportado nuevas posibilidades al atacante.

2.4.4 NECESIDADES DE SEGURIDAD

A medida que la distancia entre procesos de administración, negocio y tecnologías disminuye, el impacto de riesgo de seguridad aumenta.

Las necesidades que son fundamentales por las cuales son imperiosas las seguridades son:

- Por los riesgos que significa el tener un sistema informático en una empresa sin seguridades
- Requerimientos "legales" por parte de otras organizaciones u organismos de control
- Proceso de la información para que sea más ordenado y estandarizado

La información y los procesos, sistemas y redes que le brindan apoyo y funcionalidad constituyen importantes recursos de la empresa. La confidencialidad, integridad y disponibilidad de la información pueden ser esenciales para mantener la ventaja competitiva, el flujo de fondos, la rentabilidad, el cumplimiento de las leyes y la imagen comercial.

Las organizaciones y sus redes y sistemas de información, se enfrentan en forma creciente con amenazas relativas a la seguridad, de diversos orígenes, incluyendo el fraude asistido por computadora, espionaje, sabotaje, vandalismo, incendio o inundación. Daños tales como los ataques mediante virus informáticos, "hacking" y denegación de servicio se han vuelto más comunes, ambiciosos y crecientemente sofisticados.

La dependencia de las organizaciones respecto de los sistemas y servicios de información denota que ellas son más vulnerables a las amenazas concernientes a seguridad. La interconexión de las redes públicas y privadas y el uso compartido de los recursos de información incrementa la dificultad de lograr el control de los accesos. La tendencia hacia el procesamiento distribuido ha debilitado la eficacia del control técnico centralizado.

Muchos sistemas de información no han sido diseñados para ser seguros. La

seguridad que puede lograrse por medios técnicos es limitada y debe ser respaldada por una gestión y procedimientos adecuados. La identificación de los controles que deben implementarse requiere una cuidadosa planificación y atención a todos los detalles. La administración de la seguridad de la información, exige, como mínimo, la participación de todos los empleados de la organización. También puede requerir la participación de proveedores, clientes y accionistas. Asimismo, puede requerirse el asesoramiento experto de organizaciones externas. Los controles de seguridad de la información resultan considerablemente más económicos y eficaces si se incorporan en la etapa de especificación de requerimientos y diseño.

2.4.5 VENTAJAS Y DESVENTAJAS DE NO UTILIZARLA

La seguridad de la información, no es gratis, ni siquiera barata, pero tiene cada vez más valor para las organizaciones. Es por esto que, las inversiones en la protección de las instituciones se acrecienta continuamente.

Estructurar una defensa puede justificarse si cuesta menos que el impacto que protege. Pero no siempre es así, es necesario conocer su probabilidad. Por ejemplo, no parecería adecuado proteger el centro de proceso de información de un supermercado contra un muy improbable ataque nuclear.

Además muchas veces las ventajas obtenidas al implantar algunas defensas no son claras, pues pueden hacer más lento el funcionamiento del sistema, aumentar la burocracia, etc. hasta hacer inútiles las supuestas ventajas.

Por todo ello es necesario tener en cuenta los posibles riesgos a los que pueden enfrentarse los cuatro elementos que constituyen un sistema informático: el material físico (hardware), los componentes lógicos (software), los usuarios y la propia

información.

2.4.6 CONSIDERACIONES DE SEGURIDADES EN REDES

2.4.6.1 AMENAZAS

Existen muchos tipos de amenazas en las redes hoy en día a algunas se las ha dado un nombre pero por el motivo que crecen en forma exponencial o geométricamente no se les ha podido dar un nombre a todas pero estos son ejemplos de las que existen en la actualidad.

Atacantes	
Hacker	es una persona que batalla por la búsqueda y difusión libre de la información, la distribución sin costo del software y la globalización de la comunicación.
Crackers	son hackers cuyas intencione generalmente son con fines maliciosos o de venganza o personas que hacen daño solo por diversión.
Gurus	Son los encargados de formar y ayudar a los futuros hackers
Newbie	Son los hacker novatos
Investigadores	buscadores de reconocimiento
Deportistas	cazadores de trofeos
Criminales	
Intrusos Remunerados	Son personal contratados específicamente para robar secretos de las compañías
Personal Interno	Estos ataques son accidentes por desconocimiento o

	inexistencia de las normas básicas de seguridad
Ex – Empleado	Están interesados en violar la seguridad de la empresa por ser despedidos y no han quedado conformes con ello.
Curiosos	Tratan de vulnerar las redes no con la finalidad de hacer daño si no de obtener información prohibida
El gobierno	Tratan de vulnerar los sistemas más con la finalidad de control, y auditoria de sistemas y como un medio de obtener pruebas de alguna contravención que realicen las empresas e instituciones.
Otras fuentes de problemas	
Virus	Programas diseñados específicamente para hacer daño a los sistemas informáticos
Software defectuoso	Programas que no han seguido estándares de programación o simplemente no han seguido estándares de seguridad que pueden causar daño a los sistemas informáticos
Ataques simulados	Existen programas utilizados para simular ataques en servidores y sistemas informáticos esto puede causar que se abra agujeros en los sistemas de la organización.
Seguimiento de actualizaciones	Es necesario actualizar los sistemas para corregir los errores, posibles agujeros de seguridad, mejoramiento de los sistemas, etc.

PROBLEMAS EN AMBIENTES CLIENTE SERVIDOR	
Averiguar usuario / contraseña	Mediante técnicas de Ingeniería social se puede averiguar a usuarios incautos sus contraseñas y métodos de acceso
Robar una sesión	Mediante agujeros de seguridad se puede acceder a usuarios activos y robar su sesión
Suplantación de personalidad	Enmascarar la identidad haciendo que los registros de usuarios guarden archivos que contengan a otro usuario diferente que el original que ingreso al sistema.
Fallos en las aplicaciones	Problemas de programación al no conocer todos los posibles defectos que puede haber en el sistema por condiciones que con poca frecuencia suceden
Abuso de Privilegios	Cuando no se tiene un buen control en los privilegios de los usuarios, personal por desconocimiento o curiosidad puede causar problemas en las aplicaciones.
Fallos en los Protocolos	Los protocolos por ser abiertos no quedan exentos de virus u otros problemas en su constitución.
Otras puertas	Puertas traseras o programas sin seguridades pueden causar daños.
En los clientes	
Acceso físico al ordenador	Por parte de personas inescrupulosas acceden o roban los computadores de la empresa
Clientes Web	Los programas de traducción de codigo web son generalmente

	el principal objetivo y por los que ingresan a la red de las empresas personal no autorizado.
Sniffers	Programas que permiten capturar los paquetes que pasan por la red y si no están encriptados de alguna forma pueden servir para observar claves y documentos de los usuarios.

Tabla 2.1 AMENAZAS DE SEGURIDAD

2.4.7 CLUSTER DE SEGURIDAD

Como se menciono anteriormente en nuestro país existe una disociación entre los diferentes actores e instituciones de. la sociedad y en una compañía o institución sucede lo mismo por esta razón y aunque la norma ISO 17799 contemple la mejor organización dentro de la empresa esta no contempla lo que respecta a otras entidades fuera de ella es por esto que se ha buscado una metodología o sistema que nos permita cubrir esta necesidad con la cual estaremos en la posibilidad de tener una metodología que integra la seguridad tanto el interior de una empresa como en el entorno o medio ambiente en que se desenvuelve.

Primero se identificara cuales serán los productos o servicios que se va a ofrecer que en el caso será el de Seguridades del sitio web.

En seguida se determinará a los clientes que son las empresas e instituciones que requerirán nuestro servicio y que serán la razón de ser del servicio que se presta.

Identificaremos a nuestros proveedores que serán todas las instituciones o departamentos que nos proveen de algún objeto (servicio, información, datos, dinero, productos, hardware, software, etc.) .que nos permitirá prestar el servicio de la mejor

manera posible.

Luego se determinará a los posibles competidores que se convierten también en socios de gremio y posibles socios estratégicos de los cuales podremos aprender sus actividades exitosas emulándolas, desechando los errores y combinarlas con las estrategias de la empresa u organización que han tenido éxito teniendo como resultado mayor competitividad que los competidores.

Finalmente se determinará por separado lo que se refiere a los organismos de control los cuales nos proveen de normas y reglamentos y procesos legales los cuales los debemos conocer para cumplirlos adecuadamente.

El estado como entidad en la cual esta inmiscuida en todos los ambientes de la empresa siempre va a estar presente en cualquier cluster.

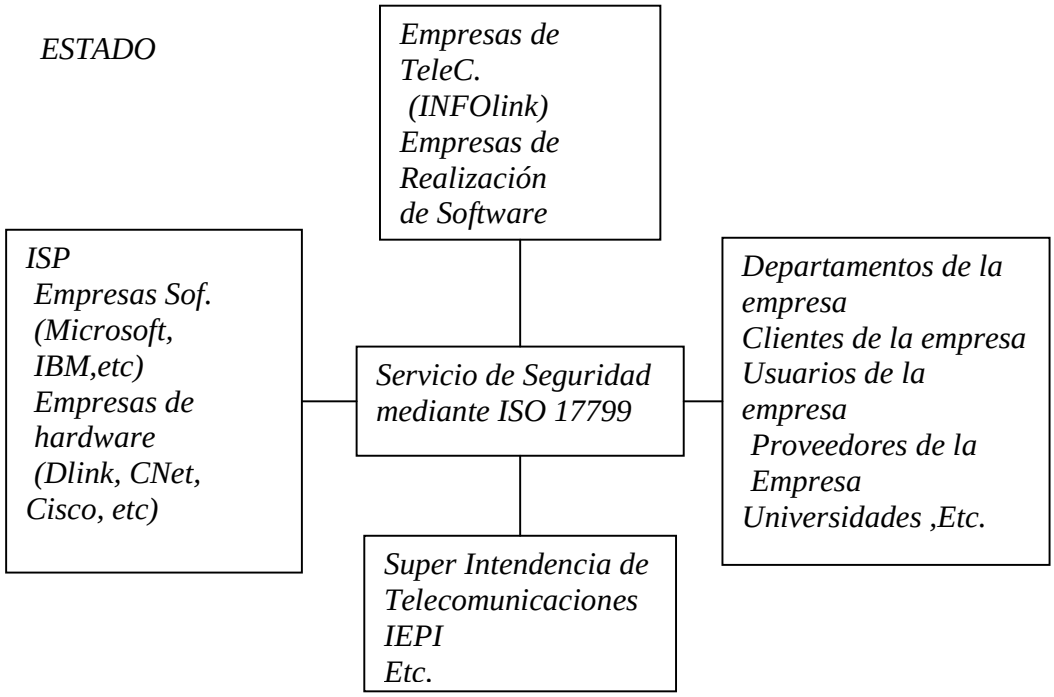
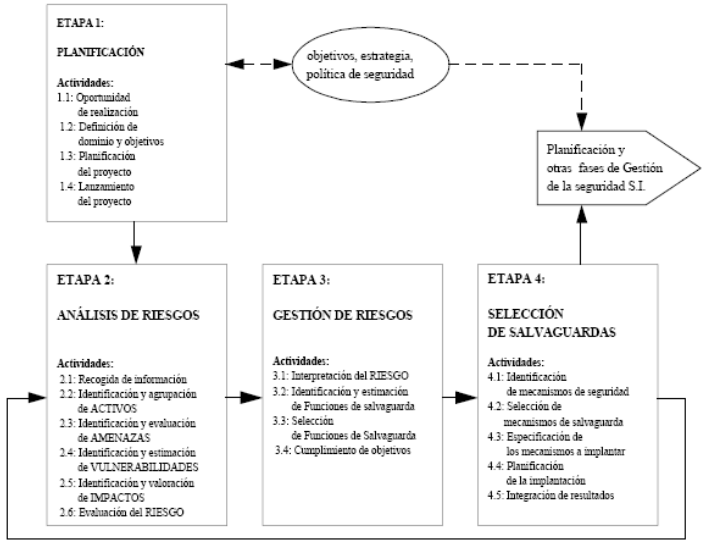


Figura 2.8 Cluster de Seguridad

2.4.8 EVALUACION Y GESTION DE RIESGOS

En la norma ISO 17799 no consta un proceso o metodología para determinar, evaluar, analizar y gestionar los riesgos de seguridad que tiene tanto la información como los medios por los cuales se distribuye, almacena además del personal que la utiliza en la empresa y fuera de ella tan solo menciona que es necesario realizarlos es por esto que se ha visto la necesidad de recurrir a la metodología MAGERIT[9] que también es utilizada para la mejora del estatus de seguridad principalmente en instituciones o empresas públicas en España pero de esta metodología se recogerá tan solo lo referente al análisis y gestión de riesgos en su forma más condensada puesto que algunas partes de esta metodología se lo realizan en algún momento en el desarrollo de la norma ISO 17799. Por lo anteriormente citado se presentará un cuadro sinóptico con los requerimientos que se especifican en la metodología MAGERIT:

2.4.8.1 VISION GLOBAL DE LAS ETAPAS DEL PROCESO MAGERIT



[9] *Magerit (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información)*

Figura 2.9 Visión Global De Las Etapas Del Proceso Magerit

2.4.8.1.1 PLANIFICACION

Es el proceso mediante el cual se presenta la iniciativa de realizar el procedimiento para obtener una gestión de riesgos adecuada hacia las personas que van a tomar la decisión de realizar o no esta tarea según los objetivos que se planteen en ese instante además de los recursos necesarios para realizarla.

2.4.8.1.2 ANALISIS DE RIESGOS

Es la estimación de las amenazas, impactos y vulnerabilidades relativos a la información y a las instalaciones de procesamiento de la misma, y a la probabilidad de que ocurran.

2.4.8.1.3 GESTION DE RIESGOS

El proceso de identificación, control y minimización o eliminación, a un costo aceptable, de los riesgos de seguridad que podrían afectar a los sistemas de información.

2.4.8.1.4 SELECCION DE SALVAGUARDAS

El proceso de selección de salvaguardas en este punto nos dará un lugar de partida para luego mediante un análisis más exhaustivo dentro del proceso de aseguramiento de la calidad por el modelo ISO17799 llegar una punto de seguridad adecuada.

2.5 LA NORMA ISO 17799

2.5.1 INTRODUCCION A LA NORMA ISO 17799

La norma ISO 17799 es una compilación de recomendaciones para las prácticas exitosas de seguridad que toda organización puede aplicar independientemente de su tamaño o sector. La norma técnica fue redactada intencionalmente para que fuera

flexible y nunca indujo a las personas que la cumplían para que prefirieran una solución de seguridad específica. Las recomendaciones de la norma técnica ISO 17799 son neutrales en cuanto a la tecnología y no ayudan a evaluar y entender las medidas de seguridad existentes.

El siguiente diagrama representa el lugar en donde se encuentra en el esquema organizacional de la empresa cada punto de la norma además contiene la subdivisión de los puntos de la ISO por el tipo de seguridad que implementan dentro de la organización sea esta legal, organizativa, física y lógica lo que nos da una pauta del personal de la empresa, departamentos, tipos de profesionales y recursos en general tanto internos como externos necesarios para el mejoramiento de la seguridad de la empresa.

Figura 2.10Puntos Que Desarrolla La ISO 17799

2.5.2 VENTAJAS DE LA NORMA TECNICA ISO 17799

Una empresa con la norma técnica ISO 17799 puede ganar frente a los competidores no apliquen la norma. Si un cliente potencial tiene que escoger entre dos servicios diferentes y la seguridad es un aspecto importante, por lo general optará por la empresa que emplee la norma. Además una empresa que utilice la norma podrá llegar a tener las siguientes beneficios:

- Mayor seguridad en la empresa.
- Planeación y manejo de la seguridad más efectivos.
- Alianzas comerciales y e-commerce más seguras.
- Mayor satisfacción y confianza en el cliente.
- Auditorias de seguridad más precisas y confiables.
- Menor Responsabilidad civil (Acceso a primas de seguro menores)
- Factor diferencial respecto de la competencia
- Responsabilidades bien diferenciadas
- Único estándar reconocido en todo el mundo
- Protección para toda la organización

2.5.3 DESVENTAJAS DE LA NORMA TECNICA ISO 17799

Así como hay muchas ventajas de emplear la norma también podemos encontrar algunas desventajas que podrían determinar

- Extenso período tanto de la discusión de la normativa, la implementación de algunas tecnologías, de la evaluación de riesgos como de otros aspectos de esta.

- Interrelación compleja con otros proyectos dentro y fuera de la empresa.
- Discusiones con proveedores de software por soluciones que se adapten a las condiciones de la ISO.
- Diferencias de criterios en clasificación de la información, de los dueños de los datos, etc.
- Algunas soluciones técnicas sólo son aplicables para todos los usuarios de todas las compañías al mismo tiempo.
- Personas “de peso” pueden decidir aplicar las políticas para todos menos para ellos.
- Dificultades en implementación de medidas disciplinarias, controles más estrictos ,etc.
- Se deja para etapas posteriores las medidas de contingencia de los equipos de procesamiento.
- Muchas de las veces se implantan los controles y puntos de la norma según el tamaño de la empresa y no respecto del tamaño, calidad y tipo de información que se debe guardar.

2.5.4 PUNTOS QUE TRATA LA NORMA

2.5.4.1 POLITICA DE SEGURIDAD

Son procesos, procedimientos, reglamentos, etc. concebidos a nivel gerencial que establece una dirección política clara y además que debe demostrar apoyo y compromiso con respecto a la seguridad de la información, mediante la formulación y mantenimiento de un documento denominado política de seguridad de la información de la institución el cual es distribuido a través de toda la organización

para el debido conocimiento de todos los integrantes de la organización y el apoyo de los mismos a este.

Las sub fases de este punto son:

- Documentación de la política de seguridad de la información
- Revisión y evaluación

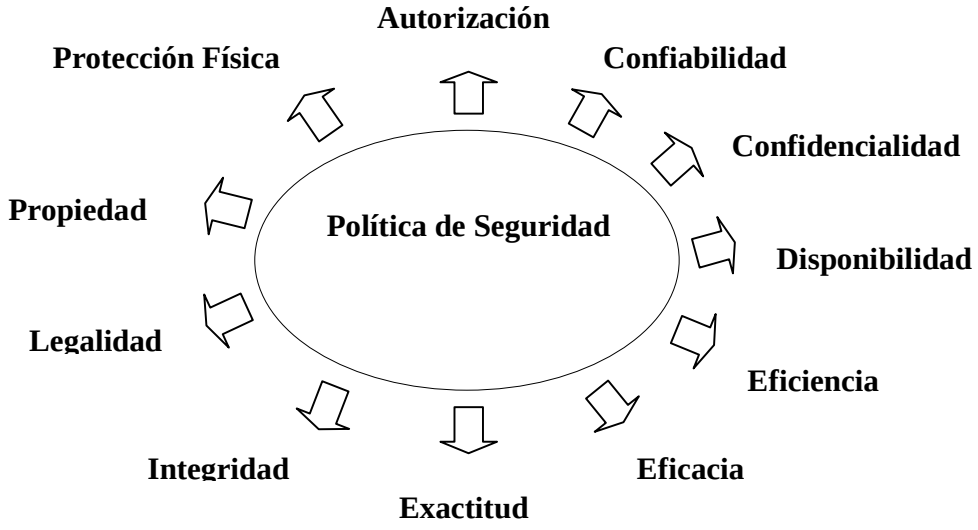


Figura 2.11 Políticas de Seguridad

2.5.4.2 ASPECTOS ORGANIZATIVOS PARA LA SEGURIDAD

Como dijimos anteriormente la seguridad no es un producto es un proceso en el cual deben estar inmersos todos los estamentos y niveles de la empresa ya que al llegar la informática hasta todas los partes de la organización, el personal de la misma debe estar inmiscuido en este concepto de lo que es seguridad puesto que como un viejo adagio dice "Una cadena es tan fuerte como su eslabón más débil" el cuál puede ser atacado por un agresor y toda la empresa debe tener en mente que reacción debe de realizar ante este ataque por lo cual se debe establecer un marco gerencial para

iniciar y controlar la implementación de la seguridad de la información dentro de la organización.

Deben establecerse adecuados foros de gestión liderados por niveles gerenciales, que deberán a más de aprobar la política de seguridad de la información, asignar funciones de seguridad y coordinar la implementación de la seguridad en toda la organización siempre teniendo en cuenta a los niveles inferiores pues su experiencia y conocimiento además de su nivel de conciencia de la organización determinan que estos sean los que nos den las pautas de cómo realizar una implantación más adecuada de la seguridad para la empresa ya que conocen como se realizan las cosas dentro de ella y saben como mejorarlas. Si resulta necesario, se debe establecer y hacer accesible dentro de la organización, una fuente de asesoramiento especializado en materia de seguridad de la información. Deben desarrollarse contactos con especialistas externos en materia de seguridad para estar al corriente de las tendencias de la industria, monitorear estándares y métodos de evaluación y proveer puntos de enlace adecuados al afrontar incidentes de seguridad. Se debe alentar la aplicación de un enfoque multidisciplinario de la seguridad de la información, por ej., comprometiendo la cooperación y colaboración de gerentes, usuarios, administradores, diseñadores de aplicaciones, auditores y personal de seguridad, y expertos en áreas como seguros y administración de riesgos.

Las sub tareas de este punto son:

- Comité de gestión de seguridad de la información.
- Coordinación de la seguridad de la información.
- Asignación de responsabilidades en materia de seguridad de la información.

- Proceso de autorización para instalaciones de procesamiento de información.
- Asesoramiento especializado en materia de seguridad de la información.
- Cooperación entre organizaciones.
- Revisión independiente de la seguridad de la información.
- Seguridad en los accesos de terceras partes.
- Identificación de riesgos por parte de terceros.
    - Tipos de acceso.
    - Motivos de acceso.
    - Subcontratados trabajando en la organización.
- Requisitos de seguridad en contratos con terceros.
- Requisitos de seguridad en contratos de outsourcing.

2.5.4.1.3 CLASIFICACION Y CONTROL DE ACTIVOS

Como dijimos anteriormente la información se ha convertido en un activo muy importante dentro de las empresas y por eso es principalmente por lo que se ha realizado esta tesis para poder conocer y buscar un conjunto de pasos, procedimientos, etc. Para poder proteger apropiadamente esta por lo cual debemos clasificarlos de acuerdo a su importancia además de determinar quien o quienes van hacer responsables de este.

Se debe rendir cuentas por todos los recursos de Información importantes y se debe designar un propietario para cada uno de ellos.

La rendición de cuentas por los activos ayuda a garantizar que se mantenga una adecuada protección. Se deben identificar a los propietarios para todos los activos importantes y se debe asignarse la responsabilidad por el mantenimiento de los

controles apropiados. La responsabilidad por la implementación de los controles puede ser delegada. En último término, el propietario designado del activo debe rendir cuentas por el mismo y esto hace que inherentemente el personal por su responsabilidad ante la empresa del activo se apropie de el y no permite el mal uso de este por terceros.

Las sub tareas de este punto son:

- Inventario de activos.
- Clasificación de la información.
    - Guías de clasificación.
    - Marcado y tratamiento de la información.

2.5.4.4 SEGURIDAD LIGADO AL PERSONAL

Uno de las variables más difíciles de predecir dentro de una empresa es el elemento humano que si se lo maneja y administra de una manera adecuada puede generar un repunte competitivo de esta pero si no puede desencadenar a la causa de errores, robo, fraude o uso inadecuado de instalaciones.

Las responsabilidades en materia de seguridad deben ser explicitadas en la etapa de reclutamiento y durante la implantación del sistema de seguridad, incluidas en los contratos y monitoreadas durante el desempeño del individuo como empleado.

Los candidatos a ocupar los puestos de trabajo deben ser adecuadamente seleccionados especialmente si se trata de tareas criticas tanto en sus conocimientos como en su calidad humana y ética. Todos los empleados y usuarios externos de las instalaciones de procesamiento de información deben firmar un acuerdo de confidencialidad (no revelación).

Las sub tareas de este punto son:

- Inclusión de la seguridad en las responsabilidades laborales.
- Selección y política de personal.
- Acuerdos de confidencialidad.
- Términos y condiciones de la relación laboral.
- Formación y capacitación en seguridad de la información.
- Comunicación de las incidencias de seguridad.
- Comunicación de las debilidades de seguridad.
- Comunicación de los fallos del software.
- Aprendiendo de las incidencias.
- Procedimiento disciplinario.

2.5.4.5 SEGURIDAD FISICA Y DEL ENTORNO

En este país donde estamos inmersos en un atraso tecnológico donde por falta de organización y por asuntos extra tecnología , que caen más en el ámbito de la política y corrupción tanto de sectores públicos como privados, se deben tomarse en cuenta otros factores como son los físicos y no solo los de organización o de software al tener que realizar un análisis más exhaustivo de la seguridad física en nuestra organización, tomando en cuenta factores como la falta de energía, los arrebatamientos de la naturaleza como son incendios, terremotos, inundaciones, etc., además del inherente elemento humano en el que se debe impedir accesos no autorizados, daños e interferencia a las redes e información de la empresa.

Las instalaciones de procesamiento de información crítica o sensible de la empresa deben estar ubicadas en áreas protegidas y resguardadas por un perímetro de

seguridad definido, con vallas de seguridad y controles de acceso apropiados. Deben estar físicamente protegidas contra accesos no autorizados, daños e intrusiones.

La protección provista debe ser proporcional a los riesgos identificados. Se recomienda la implementación de políticas de escritorios y pantallas limpios para reducir el riesgo de acceso no autorizado o de daño a papeles, medios de almacenamiento e instalaciones de procesamiento de Información.

Las sub tareas de este punto son:

- Perímetro de seguridad física.
- Controles físicos de entradas.
- Seguridad de oficinas, despachos y recursos.
- El trabajo en las áreas seguras.
- Áreas aisladas de carga y descarga.
- Instalación y protección de equipos.
- Suministro eléctrico.
- Seguridad del cableado.
- Mantenimiento de equipos.
- Seguridad de equipos fuera de los locales de la organización.
- Seguridad en el rehúso o eliminación de equipos.
- Política de puesto de trabajo despejado y bloqueo de pantalla.
- Extracción de pertenencias.

2.5.4.6 GESTION DE COMUNICACIONES Y OPERACIONES

Garantizar la operación adecuada y segura de activos (documentación de procedimientos, control de cambios, segregación, planeación y aceptación de

sistemas, código malicioso, respaldos, redes, medios de almacenamiento)

Garantizar la seguridad de la información en las redes y la protección de la infraestructura de apoyo. Es de suma importancia la administración de seguridad de las redes que pueden atravesar el perímetro de la organización.

También pueden requerirse controles adicionales para los datos sensibles que circulen por redes públicas.

Los medios de almacenamiento deben ser controlados y protegidos físicamente. Se deben establecer procedimientos operativos apropiados para proteger documentos, medios de almacenamiento (cintas, discos, casetes), datos de entrada/salida y documentación del sistema contra daño, robo y acceso no autorizado.

Las sub tareas de este punto son:

- Documentación de procedimientos operativos.
- Control de cambios operacionales.
- Procedimientos de gestión de incidencias.
- Segregación de tareas.
- Separación de los recursos para desarrollo y para producción.
- Gestión de servicios externos.
- Planificación de la capacidad.
- Aceptación del sistema.
- Medidas y controles contra software malicioso.
- Gestión interna de respaldo y recuperación.
- Recuperación de la información.
- Diarios de operación.

- Registro de fallos.
- Controles de red.
- Gestión de medios removibles.
- Eliminación de medios.
- Procedimientos de manipulación de la información.
- Seguridad de la documentación de sistemas.
- Acuerdos para intercambio de información y software.
- Seguridad de medios en tránsito.
- Seguridad en comercio electrónico.
    - Riesgos de seguridad.
    - Política de correo electrónico.
- Seguridad de los sistemas ofimáticos.
- Sistemas públicamente disponibles.
- Otras formas de intercambio de información (video, voz, fax, etc).

2.5.4.7 CONTROL DE ACCESOS

El acceso a la información y los procesos de negocio deben ser controlados sobre la base de los requerimientos, la seguridad y de los negocios. Para esta se deben tener en cuenta las políticas de difusión y autorización de la información.

Solo las personas autorizadas deben acceder a la Información o a determinado sistema que le muestre la información cruzada para poder tomar decisiones más acel1adas especialmente para los gerentes o directores. Si a esta Información pueden acceder personas no autorizadas y obtener esta, modificarla, etc. puede causar mucho malestar dentro de la organización además de posibles pérdidas para esta.

Las sub tareas de este punto son:

- Política de control de accesos.
    - Política y requisitos de negocio.
- Reglas de los controles de accesos.
- Gestión de privilegios.
- Gestión de contraseñas de usuario.
- Revisión de los derechos de acceso de los usuarios.
- Uso de contraseñas.
- Equipo informático de usuario desatendido.
- Política de uso de los servicios de la red.
- Ruta forzosa.
- Autenticación de usuarios para conexiones externas.
- Autenticación de nodos de la red.
- Protección a puertos de diagnóstico remoto.
- Segregación en las redes.
- Control de conexión a las redes.
- Control de enrutamiento en la red.
- Seguridad de los servicios de red.
- Identificación automática de terminales.
- Procedimientos de conexión de terminales.
- Identificación y autenticación del usuario.
- Sistema de gestión de contraseñas.
- Utilización de las facilidades del sistema.

- Desconexión automática de terminales.
- Limitación del tiempo de conexión.
- Restricción de acceso a la información.
- Aislamiento de sistemas sensibles.
- Registro de incidencias.
- Seguimiento del uso de los sistemas.
    - Procedimientos y áreas de riesgo.
    - Factores de riesgo.
    - Incidencias de registro y revisión.
- Sincronización de relojes.
- Informática móvil.
- Teletrabajo.

2.5.4.8 DESARROLLO Y MANTENIMIENTO DE SISTEMAS

Asegurar que la seguridad es incorporada a los sistemas de información.

Esto incluirá infraestructura, aplicaciones comerciales y aplicaciones desarrolladas por el usuario. El diseño e implementación de los procesos comerciales que apoyen la aplicación o servicio pueden ser cruciales para la seguridad. Los requerimientos de seguridad deben ser identificados y aprobados antes del desarrollo de los sistemas de Información.

Todos los requerimientos de seguridad, incluyendo la necesidad de planes de reanudación, deben ser identificados en la fase de requerimientos de un proyecto y justificados, aprobados y documentados corno una parte de la totalidad del caso de negocios de un sistema de información.

Las sub tareas de este punto son:

- Análisis y especificación de los requisitos de seguridad.
- Validación de los datos de entrada.
- Control del proceso interno.
    - Áreas de riesgo.
    - Verificaciones y controles.
    - Autenticación de mensajes.
    - Validación de los datos de salida.
- Política de uso de los controles criptográficos.
- Cifrado.
- Firmas digitales.
- Servicios de no repudio.
- Gestión de claves.
    - Protección de claves criptográficas.
    - Normas, procedimientos y métodos.
- Control del software en producción.
- Protección de los datos de prueba del sistema.
- Control de acceso a la librería de programas fuente.
- Seguridad en los procesos de desarrollo y soporte.
- Procedimientos de control de cambios.
- Revisión técnica de los cambios en el sistema operativo.
- Restricciones en los cambios a los paquetes de software.
- Canales encubiertos y código Troyano.

- Desarrollo externo del software.

2.5.4.9 GESTION DE LA CONTINUIDAD DE LOS NEGOCIOS

Diariamente escuchamos en instituciones bancarias o públicas el conocido" Se fue el sistema espere un momento por favor", este pretexto han utilizado cajeros y generalmente las personas que atienden directamente al público ya sea por la incesante pérdida de servicios, por la incompetencia de estas personas o por la sencillo desgano de querer atender a un determinado cliente pero si hubiera una adecuada administración y control de la continuidad del negocio se podría contrarrestar las interrupciones de las actividades comerciales y proteger los procesos críticos de los negocios de los efectos de fallas significativas o desastres.

Se debe implementar un proceso de administración de la continuidad de los negocios para reducir la discontinuidad ocasionada por desastres y fallas de seguridad (que pueden ser el resultado de, por ej., desastres naturales, accidentes, fallas en el equipamiento, y acciones deliberadas) a un nivel aceptables mediante una combinación de controles preventivos y de recuperación.

Se deben analizar las consecuencias de desastres, fallas de seguridad e interrupciones del servicio.

Se deben desarrollar e implementar planes de contingencia para garantizar que los procesos de negocios puedan restablecerse dentro de los plazos requeridos. Dichos planes deben mantenerse en vigencia y transformarse en un plan integral del resto de los procesos de administración y gestión.

La administración de la continuidad de los negocios debe incluir controles destinados a identificar y reducir riesgos, atenuar las consecuencias de los incidentes

perjudiciales y asegurar la reanudación oportuna de las operaciones indispensables.

Las sub tareas de este punto son:

- Proceso de gestión de la continuidad del negocio.
- Continuidad del negocio y análisis de impactos.
- Redacción e implantación de planes de continuidad.
- Marco de planificación para la continuidad del negocio.
- Prueba, mantenimiento y reevaluación de los planes de continuidad.
    - Prueba de los planes.
    - Mantenimiento y reevaluación de los planes.

2.5.4.10 CUMPLIMIENTO

Este último paso verifica el cumplimiento de los requerimientos de seguridad (legales, derechos de autor, técnicos, auditorias) antes desarrollados en la norma para luego ser evaluados y comenzar con un ciclo de mejoramiento continuo hasta tener un nivel de seguridad aceptable para la organización.

Las sub tareas de este punto son:

- Identificación de la legislación aplicable.
- Derechos de propiedad intelectual (DPI).
    - Derechos de autor.
    - Derechos de autor del software.
- Salvaguarda de los registros de la organización.
- Protección de los datos y de la privacidad de la información personal.
- Evitar el mal uso de los recursos de tratamiento de la información.
- Regulación de los controles criptográficos.

- Recopilación de pruebas.
    - Reglas para las pruebas.
    - Admisibilidad de las pruebas.
    - Calidad y totalidad de las pruebas.
- Conformidad con la política de seguridad.
- Comprobación de la conformidad técnica.
- Controles de auditoria de sistemas.
- Protección de las herramientas de auditoria de sistemas.

2.6 CONCEPTOS ADICIONALES SOBRE SEGURIDAD

2.6.1 FIREWALL

Es un sistema integrado por software, Hardware o la combinación de ambos, principalmente diseñado para administrar el uso de Internet, restringir los accesos a sitios no autorizados y lo más importante, proteger su información de ataques generalmente intentados por personas no autorizadas (externos e incluso internos) conocidas como "Hackers". Un Firewall le proporciona rep0l1es estadísticos del compol1amiento de los usuarios de la red. Información muy útil para una mejor administración.

2.6.2 IDS

Un Sistema de Detección de Intrusos o IDS *(lntrusion Detection System)* es una herramienta de seguridad encargada de monitorizar los eventos que ocurren en un sistema informático en busca de intentos de intrusión.

2.6.3 CRIPTOGRAFIA (ENCRIPTACION)

Para asegurar la transmisión de datos se han generado mecanismos a través de los

cuáles la información es codificada y decodificada por el emisor y el receptor, respectivamente. Estos se logra gracias a una sede de fórmulas matemáticas aplicadas a la información por transmitir; esto es fácil de comprender si recuerdas que en el mundo "informático" cada letra adquiere un valor numérico, de forma tal que es posible hacer operaciones matemáticas con las letras. Este tipo de acciones (llamadas cifrado) son desarrolladas y estudiadas por la criptografía.

2.6.4 SSL

El protocolo dominante en la actualidad en el panorama del comercio electrónico, proporciona confidencialidad, integridad y verificación de la identidad de ambas partes(esta últimas característica sólo si se utiliza en conjunción de cerificados digitales en ambos extremos, cosa que no suele ser frecuente).

CAPITULO III DESARROLLO DE SEGURIDADES EN CASOS PRACTICOS

3.1 INTRODUCCION

Hasta el momento la gerencia del conocimiento y de seguridad de la información ha sido aplicada en empresas con suficiente tamaño y poder como para implantar costosos proyectos dirigidos a sacarle el valor agregado al conocimiento del recurso humano. Sin embargo se plantea el problema de las PYME que, aún cuando no tienen el mismo poder que las grandes empresas, deben competir en el mismo mercado que las primeras.

La norma ISO 17799 por ser flexible se puede utilizar para mejorar la seguridad de una empresa o institución desde las más pequeñas hasta las más grandes, los sistemas informáticos más sofisticados o los más simples, la información más importante de carácter financiero como la información personal es por esto que es posible utilizarla para asegurar o mejorar la seguridad de los más diversos organismos tanto públicos como privados.

Luego de tener una visión más amplia de lo que se refiere a la gestión de seguridades en los sistemas de información y cuales son las diversas herramientas tanto físicas, lógicas, administrativas, legales, etc. que son necesarias para la mejor implementación de la norma ISO 17799 podemos determinar un proceso adecuado para su implantación.

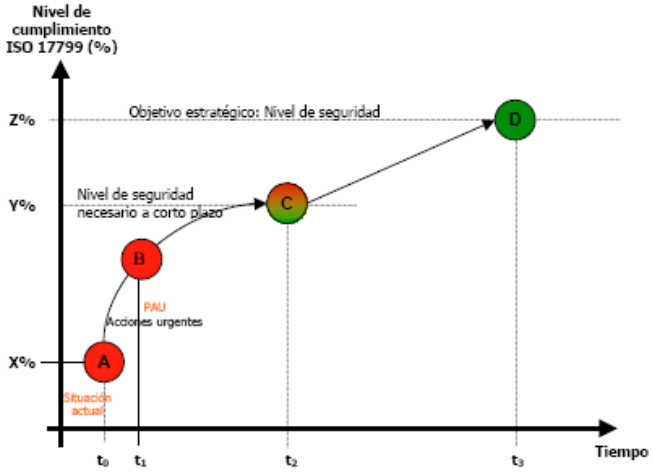


Figura 3.1 Niveles Generales de Seguridad de la Información

3.2 METODOLOGIA DE LA GESTION DE SEGURIDAD DE LA INFORMACION

Las entidades pueden organizar su estrategia de seguridad en forma de 'escalones' para mejorar su nivel progresivamente

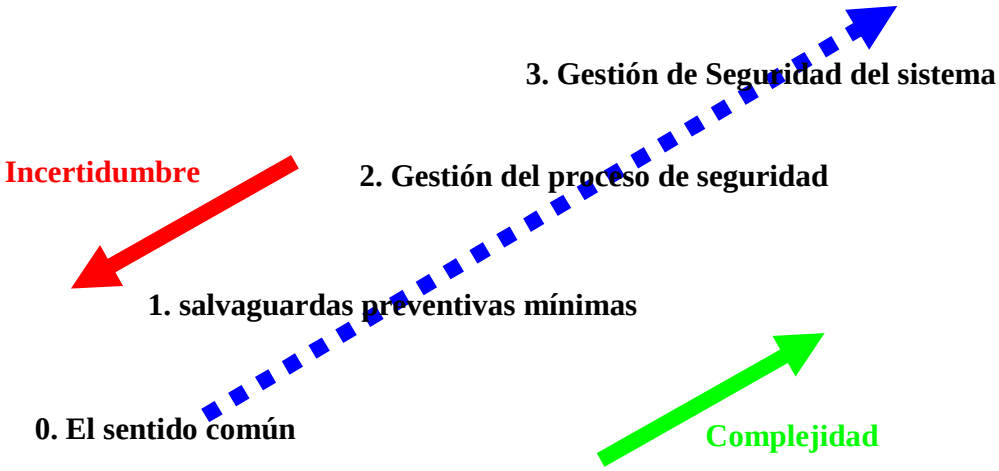


Figura 3.2 Modelo De Evolución De La Seguridad

3.2.1 ESCALON 0: EL SENTIDO COMUN

Salvaguardas, siguiendo estos Principios

- Simplicidad: atentos para detectar el peligro, sentido común para abortarlo.
- Adecuación: más vale ‘tiritas’ en la herida que vendaje ‘momia’ fuera de ella.
- Cadena: siempre se rompe por el eslabón más débil (pero hay que conocer toda la cadena del riesgo para centrarse en los puntos débiles) .
- Economía: “que no cueste más el remedio que la enfermedad”.
- Lectura de manuales, porque parte del trabajo está hecho: los sistemas comportan muchas salvaguardas; hay que reforzarlas y sistematizarlas.
- Redundancia y no-reincidencia: duplicación de espacio, no de tiempo.
- Equilibrio entre dos Peligros: Infravalorar los costes de los riesgos (o no atenderlos), supervalorar los costes de las salvaguardas (y de su instalación).
- Comodidad: salvaguardas complejas, fastidiosas, costosas no se emplean.
- Finalidad: todo problema de Seguridad termina con la instalación y uso de mecanismos de salvaguarda de varios tipos y complejidades.

3.2.2 ESCALON 1: SALVAGUARDAS PREVENTIVAS MINIMAS

Medidas de seguridad a tomar obligatoriamente

- Documento de seguridad, que contenga al menos:
  - Ámbito de aplicación con especificación detallada de los recursos protegidos.
  - Medidas, normas, procedimientos, reglas y estándares.
  - Funciones y obligaciones del personal.
  - Estructura de los ficheros y descripción de los SI que los tratan.
  - Procedimiento de notificación, gestión y respuesta ante las incidencias.

    - Procedimientos de realización de copias de respaldo y recuperación de datos.
- Documento de Funciones y obligaciones del personal.
- Identificación y autenticación de accesos autorizados.
- Registro de incidencias y procedimiento de su notificación y gestión.

Medidas adicionales si hay datos de protección media

- Procedimientos de recuperación de los datos.
- Medidas en caso de reutilización o de desecho de soportes.
- Identificación de acceso de usuarios.
- Control de acceso de usuarios.
- Gestión de soportes (identificando contenido y autorizando salida).
- Copias de respaldo y recuperación (semanales).
- Designación de responsables de seguridad.
- Control de acceso físico.
- Auditoria (cumplimiento del Reglamento, los procedimientos e instrucciones, al menos, cada dos años).

Medidas adicionales si hay datos de protección alta

- Registros de entrada y salida de soportes informáticos.
- Conservación de copia de respaldo y de los procedimientos de recuperación de los datos en un lugar distinto.
- Prohibición de pruebas con datos reales.
- Distribución de soportes (cifrado).
- Registro de accesos (usuario, hora, fichero, tipo de acceso, autorizado o no).
- Telecomunicaciones (cifrado).

3.2.3 ESCALON 2: GESTION DEL PROCESO DE SEGURIDAD

Este proceso contiene doce pasos los cuales durarán de 2 a 4 semanas cada uno dependiendo del grado de involucramiento del personal de la institución, de los recursos que se tengan disponibles, y del diagnóstico de la situación de seguridad que se encuentra la empresa.

3.2.3.1 PASO 1

- Relevar los planes de seguridad funcionales y técnicos en proceso en la compañía.
- Iniciar proceso de Identificación de Riesgos y Clasificación de Información Sensible.
- Definir el Plan de Tareas para los 2 primeros años (integrando otros proyectos de seguridad en curso).

3.2.3.2 PASO 2

- Definir, aprobar y difundir la Política de Seguridad de la Compañía.
- Definir la estructura y alcance del Manual de Seguridad de la Información de la Compañía.
- Definir y difundir las responsabilidades de Seguridad Informática de cada sector de la Compañía.
- Implementar Esquema de Propietarios de Datos.

3.2.3.3 PASO 3

- Definir e iniciar el proceso de Concientización de Usuarios internos y Terceros.
- Iniciar proceso de redacción de las Normas.

3.2.3.4 PASO 4

- Finalizar Clasificación de Información.
- Relevar medidas implementadas en las funciones del área de sistemas.

3.2.3.5 PASO 5

- Finalizar la Redacción y Difundir las Normas de Seguridad.
- Implementar las definiciones de las Normas.

3.2.3.6 PASO 6

- Implementar las mejoras de seguridad en las Funciones y Roles del área de Sistemas.
- Implementar mejoras en los sectores usuarios para información impresa.

3.2.3.7 PASO 7

- Iniciar proceso de redacción de Procedimientos críticos.
- Iniciar Programa de Continuidad del Negocio / Procesamiento Crítico de la Información.

3.2.3.8 PASO 8

- Finalizar la redacción y difundir los Procedimientos críticos.
- Dar la debida importancia al cumplimiento del Marco Legal y Regulatorio (leyes vigentes, etc).

3.2.3.9 PASO 9

- Implementar los Procedimientos de Seguridad Críticos.
- Resaltar e Integrar los Estándares Técnicos de Seguridad desarrollados dentro del Manual de Seguridad.

3.2.3.10 PASO10

- Definir junto a RRHH mecanismos de Control y Sanciones.
- Efectuar la Concientización de Usuarios de toda la Compañía.

3.2.4 ESCALON 3: GESTION DE SEGURIDAD DEL SISTEMA

En este punto se realizará un exhaustivo análisis de la empresa o institución utilizando las técnicas antes mencionadas las cuales permitirán conocer el valor real de la información y conocimiento de la misma, determinar la mejor manera de gestionarlos y protegerlos con la finalidad de convertirlos en una ventaja estratégica para dicha institución.

Tanto la gestión de conocimiento, la gestión de riesgo y el sistema de gestión de seguridad de la información son técnicas complementarias e intrínsecas entre sí que unidas darán como resultado un adecuado estatus de seguridad de la información y el conocimiento de la organización.

En la siguiente figura se pretende mostrar como se relacionan estas técnicas entre sí.

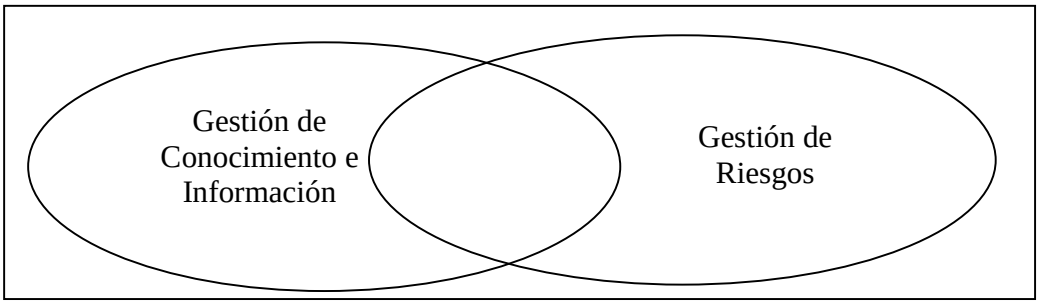


Figura 3.3 Gestión de Seguridad de la Información

La forma de obtener los mejores resultados es utilizar las técnicas antes mencionadas de la siguiente manera:

- Primero realizar La Gestión del Conocimiento e Información de la Institución.

- Luego efectuar La Gestión de los Riesgos de la misma ya que al realizar el punto anterior podemos determinar a ciencia cierta los recursos más importantes de nuestra organización.
- Finalmente mediante La Gestión de Seguridad de la Información daremos los pasos necesarios para la protección de la información de la institución.

3.2.5 CASOS PRACTICOS

3.2.5.1 INTRODUCCION

Después de haber hecho un análisis de las diferentes técnicas para el mejoramiento de la seguridad en una institución se ha establecido que:

- Para el caso de Micro empresas e industrias es suficiente el escalón cero del modelo de evolución de seguridad de la información puesto que por el número de personas y especialmente de usuarios que va a abarcar los sistemas de información, comunicaciones, etc. es mínimo, no es necesario por lo menos mientras crece la empresa hacia convertirse en pequeña empresa o hasta que su cantidad y calidad de información aumente. Sin embargo existen casos especiales de microempresas que necesitan llegar a niveles más altos en el modelo de evolución de seguridad de la información en la mayoría hasta el nivel dos pero en algunos casos pueden necesitar el nivel tres y algunos hasta la certificación, como es el caso de micro empresas e industrias de alta tecnología ejemplo: (empresas que proveen servicios de hosting de páginas web, desarrollo de software, servicios de seguridad integral de instituciones y personales, servicios de auditorias , etc).
- En el caso de Pequeñas empresas e industrias el escalón uno es suficiente ya que al igual que en el caso anterior el número de sistemas de información dentro de

una empresa de estas características es mínimo al igual que los usuarios que los utilizan o usuarios autorizados, pero al igual que el caso anterior existen excepciones en la cuales como se dijo inicialmente se debe comenzar a escalar en el modelo de evolución de seguridad de la información**.**

Por no poseer las Micro y Pequeñas empresas e Industrias la capacidad de gastar excesivamente los pocos recursos que tienen las características que debe tener las Unidades de Gerencia de Conocimiento, Riesgos y Seguridad de la información deberán ser principalmente las siguientes:

- Debe ser Económica: Debido a que la MYPE carece de poder económico para adquirir y mantener la infraestructura necesaria que tienen las grandes empresas.
- Debe Ser Simple: Al igual que la MYPE a la cual pertenece, sus procesos deben ser lo más simple posible sin sacrificar la eficacia y eficiencia.
- Debe Ser Flexible: La MYPE para poder sobrevivir, frecuentemente altera su funcionamiento regular según sus normas.
- Debe Ser Dinámica: Es necesario que sea tan dinámica como lo es la MYPE a la cual pertenece.
- Debe Ser Maleable: Considerando que la MYPE se puede expandir o contraer en tamaño, sus unidades deben ser capaz de expandirse o contraerse (según lo haga la empresa) sin disminuir la calidad de su trabajo ya que se considera fundamental en los momentos de contracción económica el sacarle el valor agregado a los recursos de la organización.

Dado la falta de recursos de las MYPE es conveniente que las mismas estén asociadas a universidades, unidades de incubación de empresas, ong’s, corporaciones, o

fundaciones en donde les ayuden a crecer y mejorar su competitividad en el mercado.

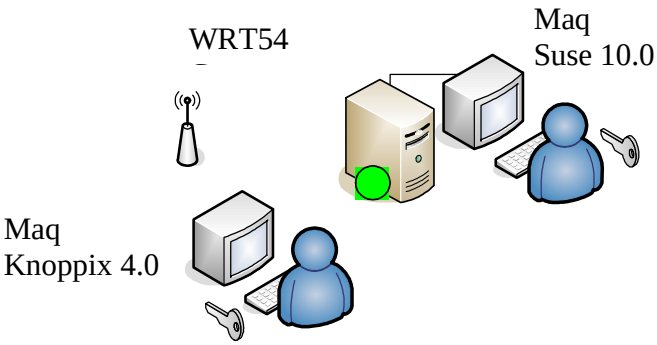
Para solventar la carencia de medios de las micro y pequeñas empresas respecto de la gestión de conocimiento, riesgos y seguridad de la información se ha visto la posibilidad de utilizar software libre el cual se ha constituido en el paradigma más utilizado en los países en vías de desarrollo para solventar la brecha tecnológica que lo separa de los estados más desarrollados.

Tomando en cuenta todos los argumentos anteriores y con la finalidad de demostrar su funcionalidad se ha escogido dos escenarios:

3.2.5.1.1 PRIMER ESCENARIO

Lo constituye un consultorio medico común en el cual generalmente se tiene un computador sub utilizado que sirve solamente para llevar el historial médico de pacientes de una forma simple utilizando hojas electrónicas.

Para mejorar las condiciones de este escenario y optimizar el tratamiento de la información se opto por el software libre Open Clinic el cual proporciona de una forma sencilla el manejo del historial médico de los pacientes tanto de un consultorio o clínica mediante una interfase web sencilla y clara para cualquier tipo de usuario sea este novato, intermedio o avanzado; cabe destacar que este programa esta realizado en el lenguaje PHP, y la base de datos esta en MySQL; se lo ha probado y configurado de acuerdo a la estructura que se presenta en el gráfico siguiente:



Leyenda		
Subtítulo de leyenda		
Símbolo	Total	Descripción
	1	Servidor Web
	3	Terminal
	3	Usuario
	3	Clave
	1	Punto de acceso inalámbrico
	1	Concentrador

Figura 3.4 Primer Escenario

En donde el servidor Web posee las siguientes características:

- Maquina Virtual
- Memoria 512MB
- Disco Duro 11GB
- Red 10/100MB
- Sistema Operativo Open Suse 10.0
- Servidor Web Apache 2.0
- Base de Datos MySQL 4.0
- Manejador de la Base de Datos PhpMyAdmin
- Manejador de servidor Webmin

Las características del cliente son las siguientes

- Maquina Virtual
- Memoria 128MB

- Disco Duro 8GB
- Red Inalámbrica USB54G
- Sistema Operativo Knoppix 4.0
- Cliente Web Firefox

Siguiendo la metodología antes indicada se podrá llegar a un mejor nivel de seguridad de este escenario mediante de la siguiente forma:

- Siguiendo lo lineamientos del Escalón 0 de la metodología en lo referente al primer punto que es la simplicidad se ha determinado que es necesario capacitar a los usuarios acerca de los diferentes mensajes, especialmente los mensajes de error que presenta los diferentes sistemas que utilizará con lo cual se aumentará su conciencia de los peligros a los que debe enfrentar y como reaccionar adecuadamente ante estos.
- En lo referente al segundo punto es necesario que se descarguen actualizaciones periódicas de los diferentes software que se utilizarán ya que mediante esta acción se minimizará las posibles agujeros de seguridad y errores que estos tengan además de impedir o disminuir la acción de las posibles amenazas anteriormente mencionadas en el documento que operen sobre estos.
- Siguiendo con los ítems del Escalón 0 podemos determinar que el eslabón más débil del escenario presentado es la demasía confianza en los diferentes artefactos utilizados en el sistema puesto que no se sigue las recomendaciones de los fabricantes acerca de mantenimiento, actualización ,seguridad ambiental y física de estos ,lo cual representa un riesgo alto en la organización, tomando conciencia

de esto podemos determinar la forma más adecuada de aminorar dicho riesgo y utilizando metodologías como son la de la teoría de las restricciones

- En lo referente a la economía que deben tener las salvaguardas que se desean implantar para el mejoramiento de las seguridades de la institución además de la utilización de software libre se debe tomar en cuenta los diferentes recursos que se utilizarán durante el desarrollo y puesta en marcha de dichas defensas o protecciones como son entre los principales el recurso humano, el recurso de tiempo, etc. Por lo antes mencionado se debe tener un apoyo de todos los integrantes de la empresa para poder realizar de una forma dual dichos salvaguardas y utilizar adecuadamente estos recursos no sobre cargándolos.
- Por la preocupación internacional acerca de la seguridad las empresas tanto de software como de hardware han implementado en sus equipos y sistemas que de manera predeterminada tengan las opciones de seguridad de los mismos habilitados con un grado mayor de protección que hasta hace algunos años con esto podemos determinar que para el siguiente item del escalón 0 además de utilizar estas configuraciones y a partir de ahí mejorar el estado de seguridad de la institución se debe documentar tanto las incidencias como las diferentes configuraciones de los equipos y sistemas de la organización para que si ocurre un desastre de seguridad en la misma la continuidad del negocio no se vea afectada minimizando el tiempo para recobrar los sistemas de la institución para el caso que se está desarrollando se presentó la configuración del sistema en conjunto en la presentación del caso.

- Siguiendo con los ítems del escalón 0 en cualquier empresa e institución se debe realizar respaldos de seguridad de la información y conocimiento más prioritaria para la continuidad del negocio los cuales en este caso será los documentos ofimáticos y las bases de datos del sistema.
- En lo concerniente al item de la Comodidad puesto que existen una cantidad de programas y metodologías para el aseguramiento de los sistemas como se mencionó con anterioridad que se utilizaría software libre para el desarrollo por su bajo o costo nulo al mismo tiempo no se utilizará tecnologías que tienen un alto costo como las biométricas o de inteligencia artificial.
- Finalmente por las condiciones que presenta el escenario antes mencionado podemos determinar que se ha escogido adecuadamente el software para el mejoramiento tanto de la gestión de la información como de las seguridades de la misma puesto que al seleccionar una distribución Linux estamos minimizando la posibilidad de virus y otras amenazas que generalmente atacan a otros sistemas operativos y programas sin embargo se recomienda utilizar antivirus tales como clamv y avg además de otras herramientas de auditoria y seguridad que se mencionarán posteriormente.

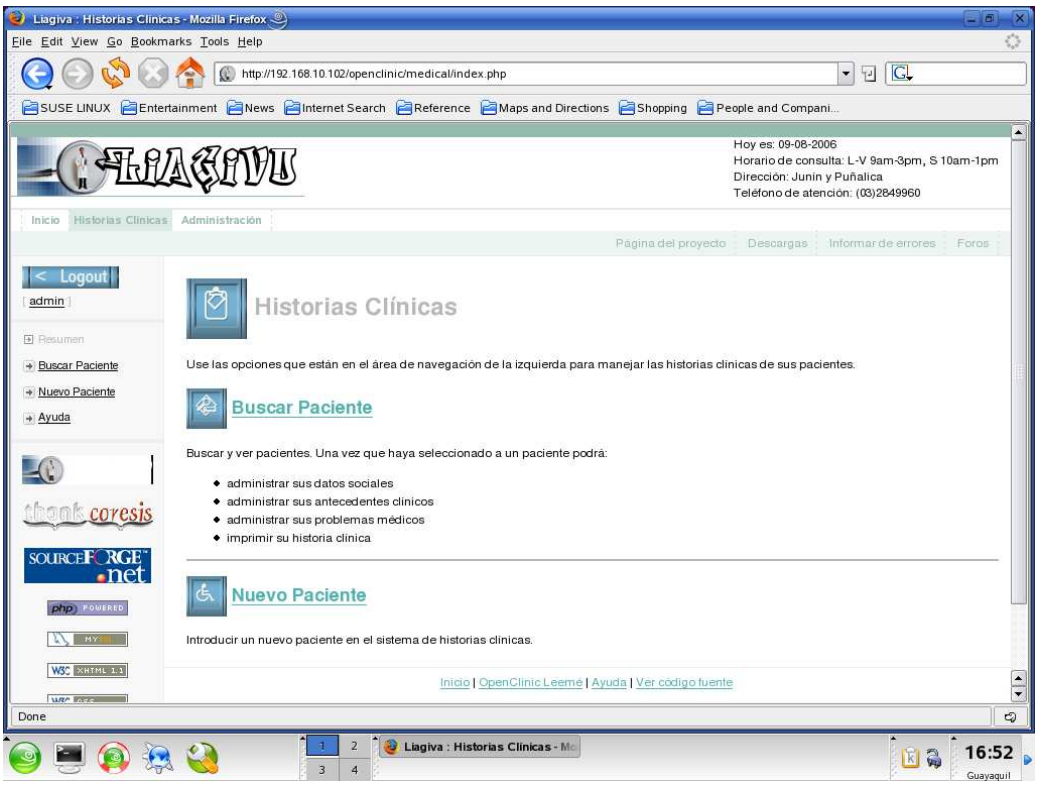


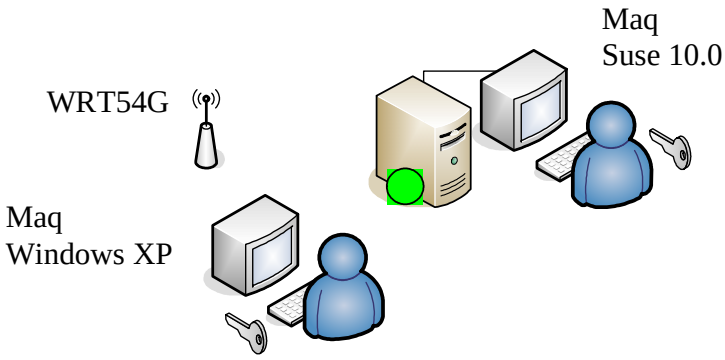
Figura 3.5 Software Openclinic

3.2.5.1.2 SEGUNDO ESCENARIO

Lo integra una institución que imparte educación; generalmente este tipo de empresas para impartir enseñanza y medir los resultados de esta, utilizan los medios tradicionales como son la toma de exámenes o pruebas escritas en papel. Para mejorar esta forma se utilizará el software libre moodle el cual permite gestionar la información antes mencionada.

Igual al caso anterior se ha escogido una interfase web por ser el medio de interacción con el computador más difundido en la actualidad además de los programas antes mencionados para el manejo tanto de las páginas web como de la base de datos y de

la información misma, como en el caso anterior se probó sus prestaciones configurando de la siguiente manera el servidor y los clientes



Leyenda		
Subtítulo de leyenda		
Símbolo	Total	Descripción
	1	Servidor Web
	3	Terminal
	3	Usuario
	3	Clave
	1	Punto de acceso inalámbrico
	1	Concentrador

Figura 3.6 Segundo Escenario

En donde el servidor Web posee las siguientes características:

- Maquina Virtual
- Memoria 512MB
- Disco Duro 11GB
- Red 10/100MB
- Sistema Operativo Open Suse 10.0
- Servidor Web Apache 2.0
- Base de Datos MySQL 4.0
- Manejador de la Base de Datos PhpMyAdmin
- Manejador de servidor Webmin

Las características del cliente son las siguientes

- Maquina Virtual
- Memoria 128MB
- Disco Duro 8GB
- Red Inalámbrica USB54G
- Sistema Operativo Windows XP
- Cliente Web Internet Explorer 6.1

A diferencia del caso anterior se ha reemplazado en la máquina cliente el sistema operativo por cuanto es más común encontrar en instituciones educativas este software además que en ellas se enseña la informática en base a dicho sistema operativo.

A semejanza del caso anterior por caer el escenario en el ámbito de una micro empresa tendrá las mismas salvaguardias que en el escenario anterior sin embargo en el punto de la adecuación es necesario que por ser el sistema Windows el escogido como cliente para este caso es necesario realizar con más frecuencia una actualización del mismo puesto que el sistema operativo Windows en sus diferentes evoluciones ha sido el software más atacado por diferentes tipos de amenazas es necesario así mimo utilizar más herramientas para protegerlo de una manera adecuada para que los posibles problemas por agresiones sean lo más tenues posibles y para ello se deberá utilizar programas antispywares, antidialers como adware, antivirus como avg , además es necesario actualizar continuamente por cuanto los agresores anteriormente definidos se aprovechan de las debilidades del software y las utilizan.

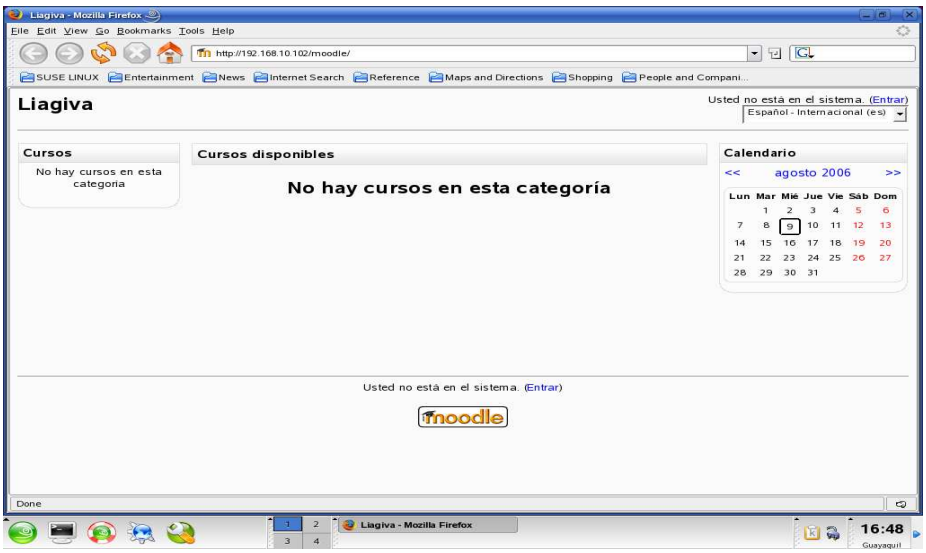


Figura 3.7 Software Moodle

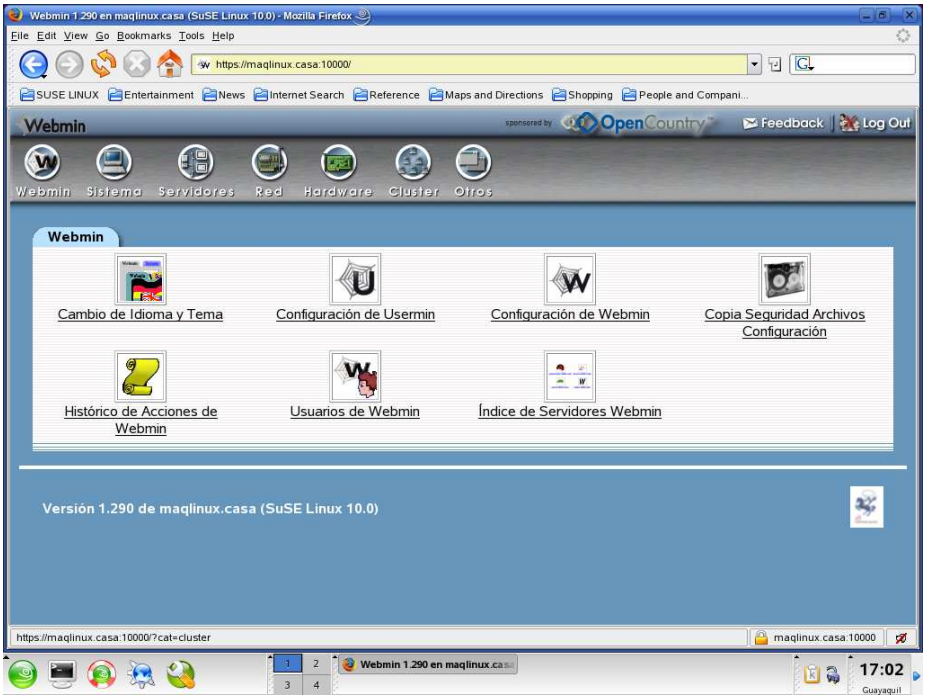


Figura 3.8 Software Webmin

CAPITULO IV CONCLUSIONES Y RECOMENDACIONES

4.1 CONCLUSIONES

- Mediante el estudio tanto de la Gestión de La Información y Conocimiento como el de La Gestión de la Seguridad de la Información ha permitido generar una metodología que permite a las empresas e industrias según sus recursos y capacidades establecer los pasos necesarios para poder escalar en la metodología generada y así como resultado tener un grado de seguridad aceptable de su información y conocimiento.
- La Gestión del Conocimiento y de la Información es un paso fundamental para el mejoramiento de una institución ya que mediante este proceso además de conocer el valor real de los recursos y capital intelectual de la organización nos da una visión más clara de las debilidades o falta de conocimiento e información que tiene la institución además concede a dicha empresa una ventaja estratégica respecto de sus iguales.
- La Gestión de Riesgos permite disminuir la incertidumbre con lo cual se da una sensación de confianza tanto al interior como al exterior de la empresa.
- La Gestión de Riesgos permite prepararnos ante cualquier amenaza y disminuir las debilidades de la empresa.
- La Gestión de Seguridad de la Información en las instituciones no es un producto si no un proceso

- La Gestión de Seguridad depende de todos los usuarios de la información y no tan solo del área informática.
- La Gestión de Seguridad de la Información se ayuda de metodologías y técnicas complementarias como son : La Gestión de la Información y Conocimiento, Gestión de Riesgos, Modelo Magerit de Análisis de Gestión de Riesgos, Clusters Administrativos, Norma ISO 17799 que permiten de forma coordinada generar un status adecuado de seguridad en la organización
- Las leyes que rigen en nuestro país no son lo suficientemente adecuadas para la protección de la información

4.2 RECOMENDACIONES

- Se aconseja a las Micro y Pequeñas empresas que sigan La Metodología antes expuesta con la finalidad de llegar gradualmente a un grado apropiado de seguridad de la información para dicha institución.
- Para determinar el nivel adecuado de seguridad para la institución principalmente debemos observar el tipo de información que queremos asegurar.
- Para un mínimo nivel de seguridad como el necesario en las micro empresas de nuestro país es tan solo necesario subir hasta el primer escalón de la metodología de gestión de seguridad de la información.
- Tanto las pequeñas y medianas empresas deben subir hasta el segundo escalón de implementación de la metodología de gestión de seguridad de la información para tener un nivel de seguridad adecuado para ellas.

- Existen normativas especiales para instituciones como Entidades Bancarias e Instituciones Médicas que sus datos necesitan un tratamiento especial de seguridad de su información pero llegando al ultimo escalón de implementación de la norma cualquier entidad llega a tener un grado adecuado de seguridad.
- Se recomienda que luego de haber realizado el estudio, análisis e implementación de las salvaguardas de acuerdo al escalón seleccionado o utilizado se realice un nuevo análisis luego de dos periodos de haber realizado el anterior estudio, entiéndase por periodo al tiempo que se utilizó para realizar todo el proceso desde el análisis hasta la implantación y puesta en marcha de las salvaguardas del sistema.
- Se recomienda para empresas que se encuentran en el proceso de la implementación de la Metodología De la Gestión Seguridad De La Información seguir los diferentes escalones de la Metodología luego de un periodo de haber realizado el escalón anterior de acuerdo al tiempo utilizado para el análisis, desarrollo y puesta en marcha del escalón anterior.
- Es recomendable que todas las instancias de la empresa estén con la predisposición para la aplicación de la metodología por cuanto para asegurar realmente la información y conocimiento útil para la misma es necesario que los implicados accedan fácilmente a compartir y sistematizar dicha información.

BIBLIOGRAFIA

INTERNET

- Autenticación y autorización

  http://www.microsoft.com/Spanish/msdn/arquitectura/BuildSecNetApps/html/

  Crear aplicaciones ASP _NET seguras, Capítulo 3 - Autenticación y autorización.htm
- Seguridad de intranet

  http://www.microsoft.com/Spanish/msdn/arquitectura/BuildSecNetApps/html/

  Crear aplicaciones ASP _NET seguras, Capítulo 5 - Seguridad de intranet.htm
- Seguridad de extranet

  http://www.microsoft.com/Spanish/msdn/arquitectura/BuildSecNetApps/html/

  Crear aplicaciones ASP _NET seguras, Capítulo 6 Seguridad de extranet.htm
- Seguridad de Internet

  http://www.microsoft.com/Spanish/msdn/arquitectura/BuildSecNetApps/html/

  Crear aplicaciones ASP _NET seguras, Capítulo 7 - Seguridad de Internet.htm
- Seguridad del acceso a datos

  http://www.microsoft.com/Spanish/msdn/arquitectura/BuildSecNetApps/html/

  Crear aplicaciones ASP _NET seguras, Capítulo 12 Seguridad del acceso a datos.htm
- Solucionar problemas de seguridad

  http://www.microsoft.com/Spanish/msdn/arquitectura/BuildSecNetApps/html/

  Crear aplicaciones ASP _NET seguras, Capítulo 13 Solucionar problemas de seguridad.htm

- La Protección de Datos Personales:Soluciones en Entornos Microsoft

  www.microsoft.com/spain/seguridad

- ISEC__Implemente_usted_mismo_ISO_17799.ppt

  www.i-sec.com.ar

- Reglamento Ley CE Corpece.zip

  www.corpece.org.ec

- IntroSegInformatica.doc

  www.uned.es

- NORMA TECNICA NTP-ISO/IEC 17799
  PERUANA 2004
  Comisión de Reglamentos Técnicos y Comerciales – INDECOPI 2004-03-05
  CAPITAL HUMANO GESTION DEL CONOCIMINETO E-LEARNING Y

  MODELOS SOCIOTECNOLOGICOS

  2006-08-31

- INTRODUCCION A LA GESTION DEL CONOCIMIENTO Y SU

  APLICACION AL SECTOR PUBLICO

  Martha Beatriz Peluffo A. y Edith Catalán Contreras

  Instituto Latinoamericano y del Caribe de Planificación Económica y Social -

  ILPES

  2002-12

- RIESGOS Y SEGURIDAD EN LOS SISTEMAS DE INFORMACION

  Julián Marcelo

  UPV-DOE

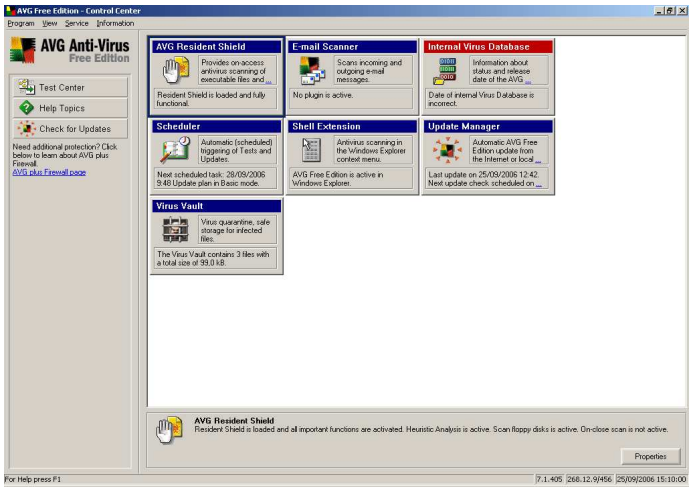
Anexos

PROGRAMAS UTILIZADOS PARA MEJORAR LA SEGURIDAD DEL SISTEMA

Adware programa Antispyware

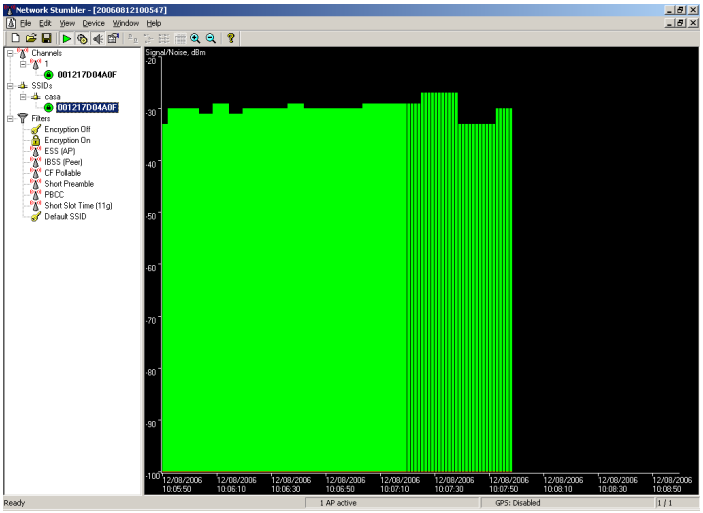
Programa que permite descubrir principalmente programas o código que tienen malas intenciones como dialers, spywares, adwares, etc

Avg Programa Antivirus



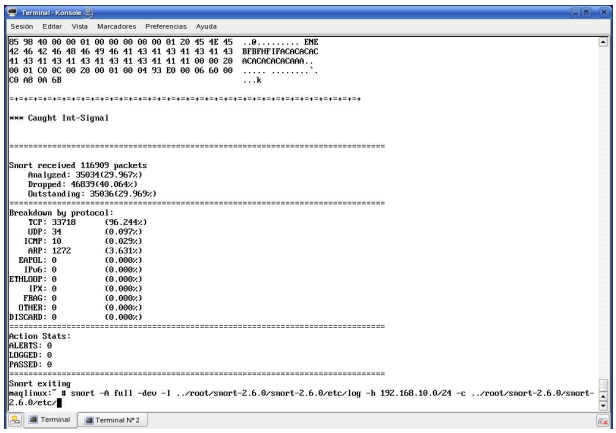
Permite escaner el computador en la búsqueda de virus informáticos

NetStumbler Programa detector de redes inalámbricas



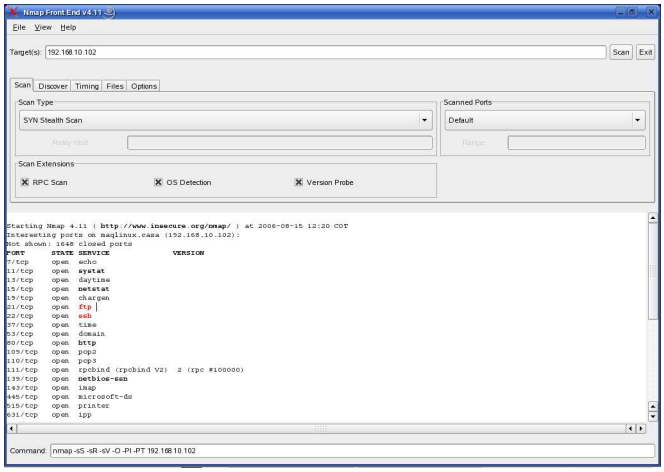
Permite además de detectar reds inalámbricas permite observar la cantidad de ruido ambiental además de localizar ,visualizar las diferentes redes al alcance además de ver que tipo de encriptación, que marca de fabricante y muchas funcionalidades más.

Snort Programa Nids y sniffer



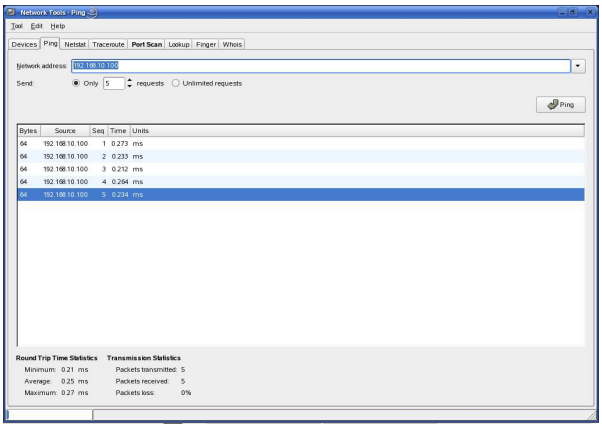
Permite además de proteger mediante alertas la integridad de la red poder acceder a los paquetes de red y mediante técnicas de sniffing obtener información de dichos paquetes.

Nmap programa escáner de puertos



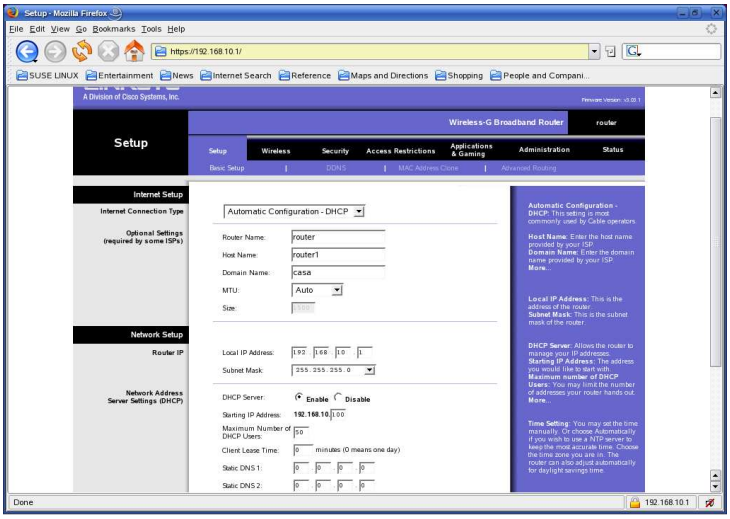
Permite escanear la red con la finalidad de detectar el estado de los puertos de un determinado computador, el nombre de las máquinas, las ip y muchas funcionalidades más.

Network Tools Programa Escaner



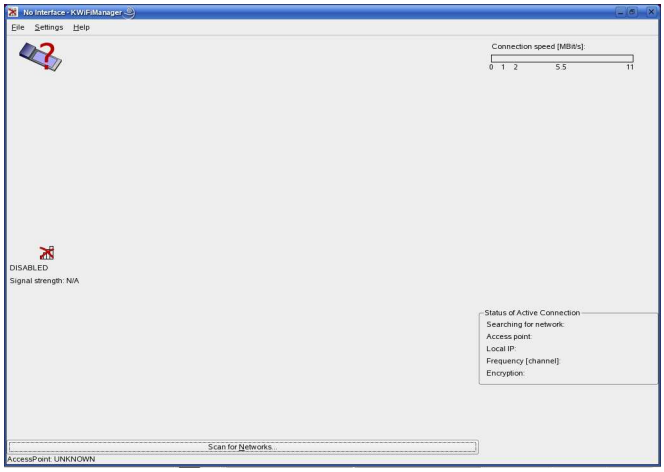
Programa gráfico que visualiza y utiliza algunos comandos útiles para administración de redes.

S.O.Linksys firmware 3.03.1



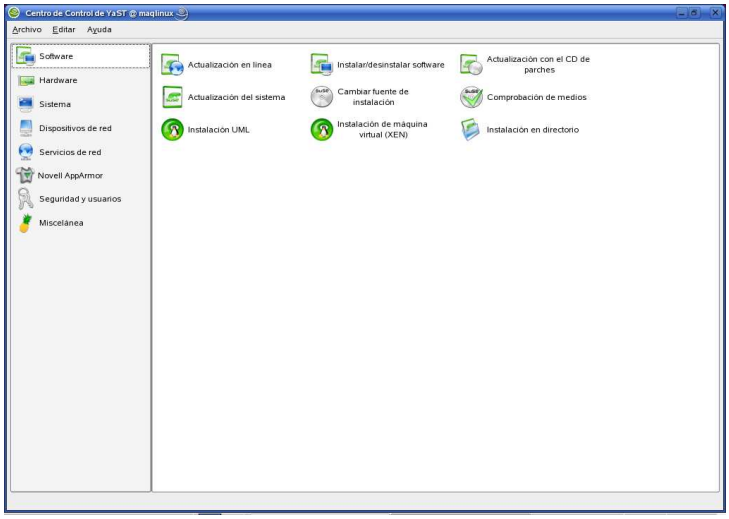
Sistema Operativo del Router Access Point Linksys, este permite configurar mediante una interfase de tipo web las características del dispositivo.

Kwifi Manager Programa Manejador De Tarjetas Wireless



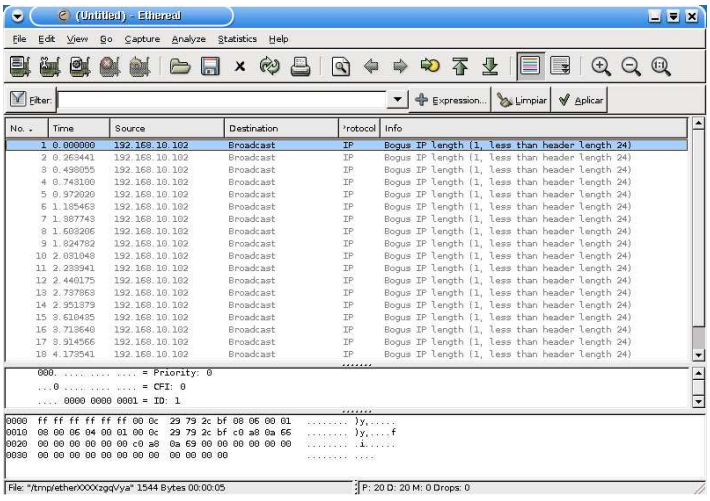
Programa manejador de tarjetas wireless en Linux, permite descubrir las redes al alcance de la tarjeta en mención además de observar la cantidad de ruido ambiental.

Yast Panel de Control



Programa visual que permite configurar dispositivos, el sistema y los diferentes servicios que tiene el sistema operativo suse 10.0

Ethereal Analizador De Paquetes



Programa que permite visualizar y analizar los paquetes que transitan por la red

LOPD

La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, protege estos datos en orden a su "tratamiento", que no es otra cosa que las operaciones y procedimientos técnicos de carácter automatizado o no que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

NIVEL BASICO: Aplicable a todos los ficheros con datos personales, nombre, dirección, teléfono, correo electrónico...

MEDIDAS DE NIVEL BASICO:

- Responsable de Fichero
- Registro de incidencias
- Listado de usuarios
- Mecanismos de identificación y autentificación
- Control de acceso
- Inventario y clasificación de soportes
- Copias de seguridad al menos semanalmente

NIVEL MEDIO: Hacienda Pública, servicios financieros, infracciones administrativas o penales, prestación de servicios de información sobre solvencia patrimonial y crédito, ficheros con datos suficientes para poder evaluar la personalidad del individuo. (Currículum, cuestionarios de evaluación del personal, etc...)

MEDIDAS NIVEL MEDIO:

- Responsable de Fichero
- Responsable de Seguridad
- Auditoria bianual
- Registro de incidencias
- Listado de usuarios
- Mecanismos de identificación y autentificación con limitación de intentos
- Control de acceso físico
- Inventario y clasificación de soportes
- Copias de seguridad

NIVEL ALTO: Datos de salud, datos policiales, datos especialmente protegidos (ideología, afiliación sindical, religión, creencias, origen racial o étnico y vida sexual).

MEDIDAS NIVEL ALTO:

- Responsable de Fichero
- Responsable de Seguridad
- Auditoria bianual
- Cifrado de soportes
- Registro de accesos, con el registro accedido
- Se conservarán dos años y se registrará una vez al mes
- Registro de incidencias
- Listado de usuarios
- Mecanismos de identificación y autentificación con limitación de intentos

- Control de acceso físico

- Inventario y clasificación de soportes

- Copias de seguridad en una ubicación diferente

RED IBEROAMERICANA DE PROTECCION DE DATOS DOCUMENTOS DE LA REDCUADRO DEL ECUADOR: DESARROLLOS NORMATIVOS NACIONALES EN MATERIA DE PROTECCION DE DATOS
(última actualización: 15.6.2004)

PAIS	**PRECEPTO CONSTITUCIONAL**	**NORMA GENERAL**	**NORMAS SECTORIALES**	**NORMAS EN PROYECTO**
ECUADOR	El numeral 8 del artículo 23 de la Constitución garantiza la intimidad personal y familiar. Su numeral 21 del artículo 23 prohíbe la utilización de la información personal de terceros referentes a sus creencias religiosas, filiación política ni sus datos sobre salud y vida sexual. El artículo 94 de la Constitución de 1998 dispone lo siguiente: "Toda persona tendrá derecho a acceder a los documentos, bancos de datos e informes que sobre sí misma, o sobre sus bienes, consten en	No existe norma general	<u>Comercio electrónico</u> **El artículo 9 de la Ley de Comercio Electró-nico protege la recopilación, cesión, uso y transmisión de datos personales obtenidos por cualquier medio y especialmente a través de bases de datos, sancionando como delito la infracción de estas disposiciones.** **<u>Estadísticas y Censo</u>** En la Ley de	No existen normas en proyecto

	entidades públicas o privadas, así como a conocer el uso que se haga de ellos y su propósito” “Podrá solicitar ante el funcionario respectivo, la actualización de los datos o su rectificación, eliminación o anulación, si fueren erróneos o afectaren ilegítimamente sus derechos. “Si la falta de atención causare perjuicio, el afectado podrá demandar indemnización “La ley establecerá un procedimiento especial para acceder a los datos personales que consten en los archivos relacionados con la defensa nacional”		Estadísticas y Censos existe la prohibición de usar información obtenida en los censos.	

REGLAMENTO GENERAL A LA LEY DE COMERCIO ELECTRONICO, FIRMAS ELECTRONICAS Y MENSAJES DE DATOS.

Artículo 1.- Incorporación de archivos o mensajes adjuntos.- La incorporación por remisión a la que se refiere el artículo 3 de la Ley 67, incluye archivos y mensajes incorporados por remisión o como anexo en un mensaje de datos a cuyo contenido se

accede indirectamente a partir de un enlace electrónico directo incluido en el mismo mensaje de datos y que forma parte del mismo.

La aceptación que hacen las partes del contenido por remisión deberá ser expresada a través de un mensaje de datos que determine inequívocamente tal aceptación. En el caso de contenido incorporado por remisión a través de un enlace electrónico, no podrá ser dinámico ni variable y por tanto la aceptación e expresa de las partes se refiere exclusivamente al contenido accesible a través del enlace electrónico al momento de recepción del mensaje de datos.

En las relaciones con consumidores, es responsabilidad del proveedor asegurar la disponibilidad de los remitidos o anexos para que sean accedidos por un medio aceptable para el consumidor cuando éste lo requiera. En las relaciones de otro tipo las partes podrán acordar la forma y accesibilidad de los anexos y remitidos.

Los anexos o remisiones referidas a garantías, derechos, obligaciones o información al consumidor deberán observar lo establecido en la Ley Orgánica de Defensa del Consumidor y su reglamento.

Toda modificación a un anexo o remitido en un mensaje de datos se comunicará al receptor del mismo, a través de un mensaje de datos o por escrito, resaltando las diferencias entre el texto original y el modificado. En el texto modificado se deberá incluir en lugar visible y claramente accesible un enlace al contenido anterior. La comunicación al consumidor acerca de modificaciones no constituye indicación de aceptación de las mismas por su parte. Dicha aceptación deberá ser expresa y remitida por cualquier medio, ya sea éste físico o electrónico.

Cuando las leyes así lo determinen, cierto tipo de información deberá estar directamente incluida en el mensaje de datos y no como anexo o remitido.

Artículo 2.- Accesibilidad de la información.- Se considerará que un mensaje de datos, sus anexos y remitidos, son accesibles para consulta posterior cuando se puede recuperar su contenido en forma íntegra en cualquier momento empleando los mecanismos y procedimientos previstos para el efecto, los cuales deberán detallarse y proporcionarse independientemente del mensaje de datos a fin de garantizar el posterior acceso al mismo.

Artículo 3.- Información escrita.- Se entiende que la información contenida en un mensaje de datos es accesible para su posterior consulta cuando:

a) Ha sido generada y puede ser almacenada en un lenguaje electrónico/informático y formato entendibles por las partes involucradas en el intercambio de información y sus respectivos sistemas informáticos de procesamiento de la información, pudiéndose recuperar su contenido y el de los remitidos o anexos correspondientes en cualquier momento empleando los mecanismos previstos y reconocidos para el efecto; y,
b) Se puede recuperar o se puede acceder a la información empleando los mecanismos previstos al momento de recibirlo y almacenarlo, y que deberán detallarse y proporcionarse independientemente el mensaje de los datos a fin de garantizar el posterior acceso al mismo.

Las publicaciones que las leyes exijan por escrito, sin perjuicio de lo establecido en dichas leyes, podrán adicionalmente efectuarse en medios electrónicos en forma de mensaje de datos.

Cumplidos los requisitos de accesibilidad, el mensaje de datos tiene iguales efectos jurídicos que los documentos que consta por escrito.

Artículo 4.- Información original y copias certificadas.- Los mensajes de datos de los documentos desmaterializados, cuando las leyes así lo determinen y de acuerdo al caso, deberán ser certificados ante un Notario, autoridad competente o persona autorizada a través de la respectiva firma electrónica, mecanismo o procedimiento autorizado.

Los documentos desmaterializados se considerarán para todos los efectos, copia idéntica del documento físico a partir del cual se generaron y deberán contener adicionalmente la indicación de que son desmaterializados o copia electrónica de un documento físico. Se emplearán y tendrán los mismos efectos que las copias impresas certificadas por autoridad competente.

Artículo 5.- Desmaterialización.- El acuerdo expreso para desmaterializar documentos deberá constar en un documento físico o electrónico con las firmas de las partes aceptando tal desmaterialización y confirmado que el documento original y que el documento desmaterializado son idénticos. En caso que las partes lo acuerden o la ley lo exija, las partes acudirán ante Notario o autoridad competente para que certifique electrónicamente que el documento desmaterializado corresponde al documento original que se acuerda desmaterializar. Esta certificación electrónica se la realiza a través de la respectiva firma electrónica del Notario o autoridad competente.

Los documentos desmaterializados deberán señalar que se trata de la desmaterialización del documento original. Este señalamiento se constituye en la

única diferencia que el documento desmaterializado tendrá con el documento original.

En el caso de documentos que contengan obligaciones, se entiende que tanto el documento original cono el desmaterializado son la expresión de un mismo acuerdo de las partes intervinientes y por tanto no existe duplicación de obligaciones. De existir multiplicidad de documentos desmaterializados y originales con la misma información u obligación, se entenderá que se trata del mismo, salvo prueba en contrario.

La desmaterialización de los documentos de identificación personal estará sujeta a las disposiciones especiales y procedimiento que las entidades competentes determinen.

Artículo 6.- Integridad de un mensaje de datos.- La consideración de integridad de un mensaje de datos, establecida en el inciso segundo del artículo 7 de la Ley 67, se cumple si dicho mensaje de datos está firmado electrónicamente. El encabezado o la información adicional en un mensaje de datos que contenga exclusivamente información técnica relativa al envío o recepción del mensaje de datos, y que no altere en forma alguna su contenido, no constituye parte sustancial de la información.

Para efectos del presente artículo, se considerará que la información consignada en un mensaje de datos es íntegra, si ésta ha permanecido completa e inalterada, salvo la adición de algún cambio que sea inherente al proceso de comunicación, archivo o presentación.

Artículo 7.- Procedencia e identidad de un mensaje de datos.- La verificación de la concordancia entre el emisor del mensaje de datos y su firma electrónica se realizará comprobando la vigencia y los datos del certificado de firma electrónica que

la respalda. En otros tipos de firmas o sistemas de identificación y autentificación, esta verificación se realizará mediante la verificación de los registros acordados o requeridos.

El aviso de un posible riesgo sobre la vulnerabilidad o inseguridad de una firma , su certificado o el mensaje de datos y los anexos relacionados podrá ser realizado por el titular de los mismos, mediante cualquier tipo de advertencia que permita, de manera inequívoca a quien realiza la verificación o recibe un mensaje de datos, tomar las precauciones necesarias para evitar perjuicios y prevenir fallas de seguridad. Este aviso deberá ser realizado antes de iniciar cualquier proceso de transacción comercial negociación o contratación electrónica

De acuerdo a las leyes, se podrá recurrir a peritos para determinar la procedencia y otro tipo de relaciones de un mensaje de datos con quien lo remite de modo directo o indirecto.

Artículo 8.- Responsabilidad por el contenido de los mensajes de datos.- La prestación de servicios electrónicos de cualquier tipo por parte de terceros, relacionados con envío y recepción de comunicaciones electrónicas, alojamiento de sitios en medios electrónicos o servicios similares o relacionados, no implica responsabilidad sobre el contenido de los mensajes de datos por parte de quien presta estos servicios, siendo la responsabilidad exclusivamente del propietario de la información.

De acuerdo a la ley y por orden de la autoridad competente, el órgano regulador podrá ordenar la suspensión del acceso a cualquier información en redes electrónicas que se declare ilegal y/o que atente contra las leyes o la seguridad nacionales. El

proveedor de servicios electrónicos deberá cumplir con la orden de suspender el acceso al contenido en forma inmediata, y en caso de no hacerlo será sancionado con sujeción a la ley por el CONELEC.

Artículo 9.- Prestación de servicios de conservación de mensajes de datos.- La conservación, incluido el almacenamiento y custodia de mensajes de datos, podrá realizarse a través de terceros, de acuerdo a lo que establece el Art. 8 de la Ley 67. los sistemas, políticas y procedimientos que permiten realizar las funciones de conservación de mensajes de datos se denominan Registro Electrónico de Datos. Una vez cumplidos los requisitos establecidos en las leyes, cualquier persona puede prestar servicios de Registro Electrónico de Datos que incluyen:

a. Conservación, almacenamiento y custodia de la información en formato electrónico con las debidas seguridades;
b. Preservación de la integridad de la información conservada;
c. Administración del acceso a la información y la reproducción de la misma cuando se requiera;
d. Respaldo y recuperación de información; y,
e. Otros servicios relacionados con la conservación de los mensajes de datos .

La prestación de servicios de Registro de Dato se realizará bajo el régimen de libre competencia y contratación. Las partes que intervengan en la contratación de este tipo de servicios, podrán determinar las condiciones que regulan su relación.

La prestación del servicio de Registro Electrónico de Datos deberá observar todas las normas contempladas en la Ley 67, este reglamento y demás disposiciones legales vigentes.

En los procesos de conservación de los mensajes de datos, se debe garantizar la integridad de los mismos al menos por el mismo tiempo que las leyes y reglamentos exijan su almacenamiento.

Por orden de autoridad competente, podrá ordenarse a los proveedores de servicios de Registro Electrónico de Datos mantener en sus sistemas respaldos de los mensajes de datos que tramite por el tiempo que se considere necesario.

Artículo 10.- Elementos de la infraestructura de firma electrónica.- La firma electrónica es aceptada bajo el principio de neutralidad tecnológica. Las disposiciones contenidas en la Ley 67 y el presente reglamento no registren la autonomía privada para el uso de otras firmas electrónicas generadas fuera de la infraestructura de llave pública, ni afecta los pactos que acuerden las partes sobre validez y eficacia jurídica de la firma electrónica conforme a lo establecido en la ley y este reglamento.

Los principios y elementos que respaldan a la firma electrónica son:

a) No-discriminación a cualquier tipo de firma electrónica, así como a sus medios de verificación o tecnología empleada;
b) Practicas de certificación basadas en estándares internacionales o compatibles a los empleados internacionalmente ;
c) El soporte lógico o conjunto de instrucciones para los equipos de computo y comunicaciones, los elementos físicos y demás componentes adecuados al uso de las firmas electrónicas, a las prácticas de certificación y a las condiciones de seguridad adicionales, comprendidas en los estándares señalados en el literal b);

d) Sistema de gestión que permita el mantenimiento de las condiciones señaladas en los literales anteriores, así como la seguridad, confidencialidad, transparencia y no-discriminación en la prestación de sus servicios; y,

e) Organismos de promoción y difusión de los servicios electrónicos, y de regulación y control de las entidades de certificación.

Artículo 11.- Duración del certificado de firma electrónica.- La duración del certificado de firma electrónica se establecerá contractualmente entre el titular de la firma electrónica y la entidad certificadora de información o quien haga sus veces. En caso de que las partes no acuerden nada al respecto, el certificado de firmas electrónicas se emitirá con una validez de dos años a partir de su expedición. Al tratarse de certificados de firma electrónica emitidos con relación al ejercicio de cargos públicos o privados, la duración del certificado de firma electrónica podrá ser superior a los dos años pero no podrá exceder el tiempo de duración de dicho cargo público o privado a menos que exista una de las prórrogas de funciones establecidas en las leyes.

Articulo 12.- Listas de revocación.- Las entidades de certificación de información proporcionarán mecanismos automáticos de acceso a listas de certificados revocados o suspendidos de acuerdo al artículo 26 de la Ley 67. Cuando la verificación de la validez de los certificados de firma electrónica no sea posible de realizar en tiempo real, la entidad de certificación de información comunicará de este hecho tanto al emisor como al receptor del mensaje de datos.

Los periodos de actualización de las listas de certificados suspendidos, revocados o no vigentes por cualquier causa se establecerán contractualmente.

Articulo 13.- Revocación del certificado de firma electrónica.- Establecidas las circunstancias determinadas en la Ley 67, se producirá la revocación, que tendrá también como consecuencia la respectiva publicación y la desactivación del enlace que informa sobre el certificado.

En caso de que las actividades de certificación vayan a cesar, la entidad de certificación deberá notificar con por lo menos noventa días de anticipación a los usuarios de los certificados de firma electrónica y a los organismos de regulación control sobre la terminación de sus actividades.

La cesión de certificados de firma electrónica de una entidad de certificación a otra, contará con la autorización expresa del titular del certificado.

La entidad de certificación que asuma los certificados deberá cumplir con los mismos requisitos tecnológicos exigidos a las entidades de certificación por la ley 67 y este reglamento.

Articulo 14.- De la notificación por extinción, suspensión o revocación del certificado de firma electrónica.- La notificación inmediata al titular del certificado de firma electrónica, de acuerdo al articulo 26 de la Ley 67, se hará a la dirección electrónica y a la dirección física que hubiere señalado en el contrato de servicio, luego de la extinción, suspensión o revocación del certificado.

Articulo 15.- Publicación de la extinción, revocación y suspensión de los certificados de firma electrónica y digital.- La publicación a la que se refiere el artículos 27 de la Ley 67, se deberá hacer por cualquiera de los siguientes medios:

a) Siempre a la página electrónica determinada por el CONELEC en la que se reporta la situación y la validez de los certificados, así como en la página WEB de la entidad certificadora; y,
b) Mediante un aviso al acceder al certificado de firma electrónica desde el hipervínculo de verificación, sea que éste forme parte de la firma electrónica, que conste en un Directorio electrónico o por cualquier procedimientos por el cual se consulta los datos del certificado de firma electrónica.

Opcionalmente en caso de que la entidad certificadora o la entidad de registro relacionada crean conveniente, se podrá hacer la publicación en uno de los medios de comunicación pública.

Articulo 16.- Reconocimiento internacional de certificados de firma electrónica.- Los certificados de firma electrónica emitidos en el extranjero tendrán validez legal en Ecuador, una vez obtenida la revalidación respectiva emitida por el CONELEC, el deberá comprobar el grado de fiabilidad de los certificados y la solvencia técnica de quien los emite.

Articulo 17.- Régimen de acreditación de entidades de certificación de información.- Para obtener autorización de operar directamente o a través de terceros relacionados en Ecuador, las entidades de certificación de información deberán registrarse en el CONELEC.

Los certificados de firma electrónica emitidos por las entidades de certificación de información que, además de registrarse, se acrediten voluntariamente en el CONELEC, tienen carácter probatorio.

Las entidades que habiéndose registrado y obtenido autorización para operar, directamente o a través de terceros relacionados en Ecuador, no se acreditan en el CONELEC, tendrán la calidad de entidades de certificación de información no acreditadas y están obligados a informar de esta condición a quienes soliciten o hagan uso de sus servicios, debiendo también, a solicitud de autoridad competente, probar la suficiencia técnica y fiabilidad de los certificados que emiten.

Articulo 18.- Responsabilidades de las entidades de certificación de información.- Es responsabilidad de la entidad certificadora de información o de la entidad de Registro que actúe en su nombre, verificar la autenticidad y exactitud de todos los datos que consten en el certificado de firma electrónica.

El CONATEL, podrá requerir en cualquier momento de la entidad de certificación de información, de la entidad de Registro que actúe en su nombre, o del titular del certificado de firma electrónica los documentos de respaldo que confirmen la autenticidad y exactitud de los datos que contiene.

Articulo 19.- Obligaciones del titular de firma electrónica.- A más de las consideradas en la Ley 67 y su reglamento, serán las mismas previstas en las leyes por el empleo de la firma manuscrita.

El órgano que ejerce las funciones de control previsto en la Ley 67, desarrollará los mecanismos, políticas y procedimientos para auditar técnicamente la actividad de las entidades bajo su control.

Articulo 20.- Información al usuario.- La información sobre los programas o equipos que se requiere para acceder a registros o mensajes de datos deberá ser proporcionada mediante medios electrónicos o materiales. En el caso de uso de

medios electrónicos se contará con la confirmación de recepción de la información por parte del usuario, cuando se usen medios materiales, los que formarán parte de la documentación que se le deberá entregar al usuario.

Para demostrar el acceso a la información el usuario deberá manifestar expresamente que conoce la información objeto de su consentimiento y que sus sistemas le permiten el acceso tecnológico a la misma.

Articulo 21.- De la seguridad en la prestación de servicios electrónicos.- La prestación de servicios electrónicos que impliquen el envío por parte del usuario de información personal, confidencial o privada, requerirá el empleo de sistemas seguros en todas las etapas del proceso de prestación de dicho servicio. Es obligación de quien presta los servicios, informar en detalle a los usuarios sobre el tipo de seguridad que utiliza, sus alcances y limitaciones, así como sobre los requisitos de seguridad exigidos legalmente y si el sistema puesto a disposición del usuario cumple con los mismos. En caso de no contar con seguridades se deberá informar a los usuarios de este hecho en forma clara y anticipada previo al acceso a los sistemas o a la información de instruir claramente sobre los posibles riesgos en que pueden incurrir por la falta de dichas seguridades.

Se consideran datos sensibles del consumidor sus datos personales, información financiera de cualquier tipo como números de tarjetas de crédito o similares que involucren transferencias de dinero o datos a través de los cuales puedan cometerse fraudes o ilícitos que le afecten.

Por el incumplimiento de las disposiciones contenidos en el presente artículo o por falta de veracidad o exactitud en la información sobre seguridades, certificaciones o

mecanismos para garantizar la confiabilidad de las transacciones o intercambio de datos ofrecida al consumidor o usuario, el organismo de control podrá exigir al proveedor de los servicios electrónicos la rectificación necesaria y en caso de reiterarse el incumplimiento o la publicación de información falsa o inexacta, podrá ordenar la suspensión del acceso al sitio con la dirección electrónica del proveedor de servicios electrónicos mientras se mantengan dichas condiciones.

Artículo 22.- Envió de mensajes de datos no solicitados.- El envío periódico de información, publicidad o noticias promocionando productos o servicios de cualquier tipo observará las siguientes disposiciones:

a. Todo mensaje de datos periódico deberá incluir mecanismos de suscripción y de suscripción;
b. Se deberá incluir una nota indicando el derecho del receptor a solicitar se le deje de enviar información no solicitada;
c. Deberá contener información clara del remitente que permita determinar inequívocamente el origen del mensaje de datos;
d. A solicitud del destinatario se deberá eliminar toda información que de él se tenga en bases de datos o en cualquier otra fuente de información empleada para el envió de mensajes de datos periódicos u otros fines no expresamente autorizados por el titular de los datos.
e. Inmediatamente de recibido por cualquier medio la solicitud del destinatario para suscribirse del servicio o expresando su deseo de no continuar recibiendo mensajes de datos periódicos, el emisor deberá cesar el envío de los mismos a la dirección electrónica correspondiente.

Las solicitudes de no envío de mensajes de datos periódicos, se harán directamente por parte del titular de la dirección electrónica de destino.

Los proveedores de servicios electrónicos o comunicaciones electrónicas, a solicitud de cualquiera de sus titulares de una dirección electrónica afectado por el envió periódico de mensajes de datos no solicitados, procederán a notificar al remitente de dichos correos sobre el requerimiento del cese de dichos envíos y de comprobarse que el remitente persiste en enviar mensajes de datos periódicos no solicitados podrá bloquear el acceso del remitente a la dirección electrónica afectada.

Articulo 23.- Sellado de tiempo.- Para la prestación de los servicios de sellado de tiempo, el mensaje de datos debe ser enviado a través de la entidad certificadora o un tercero debidamente registrado en el CONELEC para prestar este servicio. El sellado de tiempo únicamente establecerá para los fines legales pertinentes, la hora y fecha exacta en que el mensaje de datos fue recibido por la entidad certificadora o el tercero registrado por el CONELEC; y la fecha y hora exacta en dicho mensaje de datos fue entregado al destinatario.

Para efectos legales el servicio de sellado de tiempo se prestará tomando como referencia el huso horario del territorio continental ecuatoriano.

La prestación de servicios de sellado de tiempo se realizará en régimen de libre competencia y contratación. Las partes que intervengan en la contratación de este tipo de servicios podrán determinar las condiciones que regulen su relación.

LEY DE PROPIEDAD INTELECTUAL

DE LOS DERECHOS DE AUTOR Y DERECHOS CONEXOS

CAPITULO I

Del Registro Nacional de Derechos de Autor y Derechos Conexos

Art. 7.- El Registro Nacional de Derechos de Autor y Derechos Conexos estará a cargo de la Dirección Nacional de Derechos de Autor y Derechos Conexos del IEPI.

Art. 8.- En el Registro Nacional de Derechos de Autor y Derechos Conexos se inscribirán obligatoriamente:

a) Los estatutos de las sociedades de gestión colectiva, sus reformas, su autorización de funcionamiento, suspensión o cancelación; b) Los nombramientos de los representantes legales de las sociedades de gestión colectiva;

c) Los convenios que celebren las sociedades de gestión colectiva entre sí o con entidades similares del extranjero; y,

d) Los mandatos conferidos en favor de sociedades de gestión colectiva o de terceros para el cobro de las remuneraciones por derechos patrimoniales.

Art. 9.- En el Registro Nacional de Derechos de Autor y Derechos Conexos podrán facultativamente inscribirse:

a) Las obras y creaciones protegidas por los derechos de autor o derechos conexos;

b) Los actos y contratos relacionados con los derechos de autor y derechos conexos; y,

c) La transmisión de los derechos a herederos y legatarios.

Art. 10.- Las inscripciones a que se refiere el artículo 9 del presente Reglamento tienen únicamente valor declarativo y no constitutivo de derechos; y, por consiguiente, no se las exigirá para el ejercicio de los derechos previstos en la Ley.

Art. 11.- La resolución del Director Nacional de Derechos de Autor y Derechos Conexos que apruebe los estatutos de una sociedad de gestión colectiva o sus reformas, o que autorice su funcionamiento, dispondrá su inscripción en el Registro Nacional de Derechos de Autor a la que acompañará 2 ejemplares y el comprobante del pago de la tasa respectiva.

El Director Nacional de Derechos de Autor y Derechos Conexos, en los casos de suspensión o cancelación de personería jurídica de una sociedad de gestión dispondrá la inscripción de esta resolución en el Registro Nacional de Derechos de Autor y Derechos Conexos.

Art. 12.- Los nombramientos de los representantes legales de las sociedades de gestión colectiva, los convenios que celebren dichas sociedades de gestión entre sí o con similares en el exterior, y los mandatos conferidos a su favor o a favor de terceros para el cobro de las remuneraciones por derechos patrimoniales se inscribirán con la sola presentación de tales documentos.

Art. 13.- La solicitud de inscripción de una obra contendrá:

a) Título de la obra;

b) Naturaleza y forma de representación de la obra; y,

c) Identificación y domicilio del autor o autores.

Art. 14.- A la solicitud de inscripción de una obra se acompañarán, según el caso, dos ejemplares de la obra o de los medios que permitan apreciarla y el comprobante de pago de la tasa respectiva.

El solicitante podrá, a fin de mantener la reserva sobre información controlada, depositar las fijaciones u otros medios que incorporen prestaciones protegidas ante un Notario Público.

Art. 15.- Los actos y contratos de transferencia de derechos patrimoniales se inscribirán con la sola presentación, una vez que se haya acreditado el pago de la tasa correspondiente.

Art. 16.- Las inscripciones de que trata este Capítulo se otorgarán a la sola presentación de la solicitud que contenga los requisitos señalados y los ejemplares de la obra o los medios que permitan apreciarla.

Art. 17.- El Director Nacional de Derechos de Autor y Derechos Conexos determinará los libros de inscripciones que serán llevados en el Registro Nacional de Derechos de Autor y Derechos Conexos.