UNIVERSIDAD CENTROCCIDENTAL
"LISANDRO ALVARADO"

ANÁLISIS DE LOS RIESGOS DE SEGURIDAD INFORMÁTICA, PARA LAS PEQUEÑAS Y MEDIANAS EMPRESAS (PYME'S) USANDO EL ESTÁNDAR ISO-17799, PARA LA DEFINICIÓN DE POLÍTICAS DE SEGURIDAD QUE PROTEJAN SUS SISTEMAS DE INFORMACIÓN

FABIOLA VILLASMIL

Barquisimeto, 2006

UNIVERSIDAD CENTROCCIDENTAL
"LISANDRO ALVARADO"
DECANATO DE CIENCIAS Y TECNOLOGÍA
COORDINACIÓN DE POSTGRADO

ANÁLISIS DE LOS RIESGOS DE SEGURIDAD INFORMÁTICA, PARA LAS PEQUEÑAS Y MEDIANAS EMPRESAS (PYME'S) USANDO EL ESTÁNDAR ISO-17799, PARA LA DEFINICIÓN DE POLÍTICAS DE SEGURIDAD QUE PROTEJAN SUS SISTEMAS DE INFORMACIÓN

Trabajo presentado para optar al grado de Técnico Superior
Especialista en Tecnologías de la Información y comunicaciones

Por: FABIOLA VILLASMIL

Barquisimeto, 2006

ANÁLISIS DE LOS RIESGOS DE SEGURIDAD INFORMÁTICA, PARA LAS PEQUEÑAS Y MEDIANAS EMPRESAS (PYME'S) USANDO EL ESTÁNDAR ISO-17799, PARA LA DEFINICIÓN DE POLÍTICAS DE SEGURIDAD QUE PROTEJAN SUS SISTEMAS DE INFORMACIÓN

Por: FABIOLA VILLASMIL

Trabajo de Grado Aprobado

_____ **Jurado 1**

_____ **Jurado 2**

_____ **Jurado 3**

Barquisimeto, _____ de _____ del 200__

AGRADECIMIENTOS

A Dios Padre Todopoderoso.

A mi Mamá, por darme vida, respaldo y compresión.

Ana Karina, Rafael y Elba Marina, por su constancia, tolerancia y su valioso apoyo incondicional.

A todos mis amigos personales, que siempre me brindaron su ayuda.

A la Profesora Mailen por su colaboración, orientación y cooperación

A mis profesores, por su disposición y excelente colaboración

A la Cámara de Pequeños y Medianos Industriales del Estado Lara (CAPMIL), por su valiosa colaboración.

INDICE DE CUADROS

INDICE DE FIGURAS

INDICE DE GRÁFICOS

UNIVERSIDAD CENTROCCIDENTAL
"LISANDRO ALVARADO"
DECANATO DE CIENCIAS Y TECNOLOGÍA
COORDINACIÓN DE POSTGRADO

ANÁLISIS DE LOS RIESGOS DE SEGURIDAD INFORMÁTICA, PARA LAS PEQUEÑAS Y MEDIANAS EMPRESAS (PYME'S) USANDO EL ESTÁNDAR ISO-17799, PARA LA DEFINICIÓN DE POLÍTICAS DE SEGURIDAD QUE PROTEJAN SUS SISTEMAS DE INFORMACIÓN

Autor (a): Fabiola Villasmil
Tutor (a): Msc. Mailen Camacaro

RESUMEN

La investigación tiene como propósito el Análisis de Riesgos en Seguridad Informática en las Pyme's de la Zona Industrial de Barquisimeto, para la definición de políticas de seguridad, que permitan proteger sus sistemas de información, usando el estándar ISO-17799. Para lo cual se plantearon los objetivos de identificar las situaciones de riesgo que afecten la seguridad informática de este grupo empresarial, además de determinar cuales son las herramientas de control para reducir y monitorear dichos riesgos, asimismo la propuesta de un conjunto de lineamientos basados en el estándar ISO-17799, que permitan establecer políticas de seguridad para los sistemas de información de las PyME's. El tipo de investigación es de campo, no experimental, descriptiva, con el objetivo de analizar riesgos de seguridad informática en la PyME, por consiguiente, se utiliza un instrumento de recolección de datos, que se aplica a los administradores de los sistemas de información dentro de las empresas seleccionadas, la información recaudada, se analiza desde el punto de vista estadístico, para la presentación de los resultados de la investigación se utilizan gráficos, que detallan los datos obtenidos y permiten su análisis, finalizando con una serie de conclusiones y recomendaciones, que están orientadas a mejorar el desempeño de los sistemas de información en las PyME's.

Palabras clave: seguridad de la Información, riesgos informáticos, políticas de seguridad, estándares de seguridad.

INDICE GENERAL **Pág.**

INTRODUCCIÓN

El mundo actual cada vez más globalizado, exige de parte de las empresas un mayor y mejor acceso a la información, esto con el objetivo de mejorar sus relaciones con clientes, proveedores, empleados. Las tecnologías de la información, han abierto una serie de posibilidades para las pequeñas y grandes empresas, dándoles nuevas oportunidades dentro de sus mercados y haciéndolas más competitivas.

Ante estos nuevos cambios tecnológicos, también aparecen los riesgos y el problema de contar con una plataforma informática segura. Una forma de enfrentar los problemas de seguridad de la información que se presentan en la actualidad, es que las empresas entiendan lo importante, que es proteger sus sistemas de información de intrusos, usuarios o daños fortuitos, que pongan en peligro el desempeño informático de la empresa.

La velocidad con que ocurren los cambios, sobre todo en el área tecnológica, hace difícil la planeación estratégica, que permita asegurar el capital intelectual representado por la información dentro de una empresa. Por lo que hace necesario integrar las estrategias de negocio con las estrategias tecnológicas en materia informática, lo que traerá como consecuencia un diseño e implementación de políticas de seguridad que se ajusten a la organización.

La seguridad de la información, involucra la protección de los activos de la información. Para lo cual es necesario identificar las situaciones de riesgo que se puedan determinar, cuales de estos activos son vulnerables ante las amenazas, tanto internas, como externas a la empresa. Tomando en cuenta que entre los objetivos de la seguridad de la información, se encuentran el acceso, confiabilidad e integridad de la información, es necesario determinar que herramientas o controles pueden ayudar, reducir y a monitorear los riesgos detectados en las plataformas informáticas empresariales. Entre este tipo de controles se cuentan las políticas o normas de seguridad para el

manejo de la información tales como, la adopción del estándar ISO-17799. En este documento se especifican las reglas para el uso de la información dentro de una organización, además establece los planes de continuidad del negocio, en caso de fallas o problemas con la información, con el propósito de aminorar los riesgos informáticos más probables.

Por consiguiente, la seguridad informática esta estrechamente relacionada con los procesos de negocio. Por lo tanto es la gerencia de una organización, la que aporta las estrategias para la administración eficiente de las tecnologías de la información, que permitan el aseguramiento de la información.

En el capitulo I de la presente investigación se hace el planteamiento del problema, exponiendo la situación que dio origen al estudio, además se establecen los objetivos de la investigación, seguido de la justificación y el alcance propuesto. En el capitulo II, se constituyen las bases teóricas para el estudio, mencionando los antecedentes relacionados con la investigación, conceptos importantes ligados a la seguridad informática y riesgos informáticos, así como la descripción del estándar ISO-17799 para la seguridad de la información, culminando con la operacionalización de variables diseñado para la investigación. El capitulo III, trata el aspecto metodológico, donde se expone el tipo de investigación que se hará, así como la población y muestra del estudio propuesto, además de la técnica para recolección de datos y presentación de la información. En el capitulo IV, se presenta los resultados del estudio, los cuales se hacen a través de gráficos, seguido del análisis, donde se selecciono el mayor numero de frecuencia por los ítems planteados en el instrumento de recolección de datos, para concluir la investigación se presenta el capitulo V, donde se exponen las conclusiones y recomendaciones del estudio propuesto.

CAPITULO I
EL PROBLEMA

Este capitulo trata sobre el planteamiento del problema, que será objeto de la investigación. Se relatará de forma breve las situaciones que dan origen al tema seleccionado por el investigador para la elaboración de este trabajo, asimismo, se formulan el objetivo general y los objetivos específicos, además de la justificación del problema y su alcance.

Planteamiento del Problema

El mundo actual, cada vez más competitivo y exigente, motivado al auge de la globalización, ha creado la necesidad en las empresas de gestionar adecuada y oportunamente la información, que producen. Para la transformación de dicha información, se originan los Sistemas de información, los cuales se basan en su definición.

Laundon (2002), señala: que un sistema de información, es un grupo de componentes interrelacionados que trabajan en conjunto, para procesar, almacenar y distribuir información, que sirva para la toma de decisiones y control dentro de una organización.

Con referencia a lo anterior O'Brien (2001), plantea un concepto adecuado para el medio informático, refiriéndolo como una combinación organizada de personas, hardware, software, redes de comunicaciones y recursos de datos, que reúnen, transforman y diseminan información en una organización. El mismo menciona que en la actualidad ninguna organización puede prescindir de un sistema de información que apoye su gestión, porque la organización como tal es un sistema.

En tal sentido, los sistemas de información se han convertido en parte crucial de las actividades empresariales, gubernamentales, académicas y cotidianas. Donde la información adquiere mayor importancia y requiere del tratamiento adecuado para su aprovechamiento. De allí surge la necesidad de protegerla y asegurarse que sea precisa y confiable. La información es algo intangible, que se concentra dentro de los sistemas de información, la cual puede: almacenarse dentro de archivos de computadoras, transmitirse a través de redes computacionales, registrarse en papel o en cualquier soporte de datos digital para su movilización.

Según Laudon (2002), los datos automatizados (digitales) son más propensos a destrucción, fraude, error o abuso por parte de personas no autorizadas. Además, agrega que la falla de un sistema de información o un funcionamiento indebido del mismo, produce en las organizaciones que dependen de ellos, grandes y graves pérdidas de su capacidad de operación.

Tal como se observa, la seguridad informática se refiere, al establecimiento de políticas para administrar y controlar eficientemente el funcionamiento de un sistema de información, que permitan protegerlo del acceso de personas no autorizadas, alteración de datos o daños físicos a su plataforma tecnológica.

Oz (2001), expresa que la seguridad informática puede verse afectada seriamente por los cambios organizacionales de la actualidad, cuando la mayoría de las empresas ha comenzado a aumentar sus actividades o negociaciones en línea, ya sea en Internet o través de Intranets o Extranets.

Ramió (2006), La define en su libro: Seguridad informática y criptología como: “Un conjunto de métodos y herramientas destinados a proteger la información y por ende los sistemas informáticos ante cualquier amenaza, un proceso en el cual participan además las personas”. Hoy en día se aborda la seguridad de los sistemas de información de forma integral, teniendo en cuenta la complejidad de las comunicaciones y la variedad de los servicios que deben ofrecer dichos sistemas.

El Consejo Superior de Informática de España plantea en sus Guías técnicas sobre seguridad informática, que el objeto de la misma, es asegurar que la información sea autentica, confidencial, integra y que este disponible cuando se le requiera.

Partiendo de esta definición encontramos que existen varios tipos de seguridad informática. La seguridad física se refiere al aseguramiento de todos los componentes físicos (hardware), que necesitan los sistemas de información para su correcto funcionamiento. La seguridad lógica (software) esta asociada con la protección de la información o datos, procesos, programas y la determinación del acceso autorizado hacia los mismos. Adicionalmente, se encuentra la seguridad organizacional, referida a las acciones que toman los directivos de una organización para la adecuada gestión y protección de la información que producen, almacenan, y/o transmiten los sistemas de información que apoyan las operaciones de su organización. De igual manera esta la seguridad informática desde el punto de vista legal, la cual esta relacionada con normativas jurídicas que establece cada nación para el tratamiento de la información electrónica o digital, esta persigue el aseguramiento de los datos o información desde la perspectiva legal.

Actualmente la seguridad informática es un tema de honda preocupación a nivel internacional, debido al aumento de los procesos de apertura económica, el comercio global sobre todo a través de los medios electrónicos, han incrementado los problemas de seguridad de la información para las organizaciones.

Por otra parte, Hernando (2005), considera que hoy día ninguna organización, puede carecer de mecanismos de protección para la plataforma tecnológica que sustenta sus sistemas de información. Algunas invierten más dinero que otras en seguridad informática, pero todas necesitan del aseguramiento de sus datos, para garantizar su funcionamiento operacional.

Países como España, México, Chile, Argentina, trabajan arduamente para el establecimiento de políticas de gestión de la seguridad informática que permitan disminuir el riesgo o vulnerabilidad de la información administrada por los sistemas de información de sus organizaciones. De estos, España es uno de los más avanzados en el tema; el gobierno español ha creado normativas que permiten orientar las políticas de seguridad de la información, a través del Real decreto 263/1996, que versa sobre la regulación de la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado (España). A nivel internacional existen una serie de normativas estándares que se aplican para los procesos de establecimiento de seguridad informática en las organizaciones. Las principales relacionadas con la seguridad de los Sistemas de información son las siguientes:

- El estándar ISO 17799, es una norma internacional que ofrece recomendaciones para realizar la gestión de seguridad de la información en las organizaciones, permitiéndoles establecer un marco de seguridad para los activos de la información.
- El estándar ISO 7498-2 (OSI, Security Architecture), describe el modelo de referencia ISO/OSI.
- El TCSEC (Trusted Computer Security Evaluation Criteria) definidas por el Departamento de Defensa de EEUU (conocido como el Libro Naranja). Suministra especificaciones de seguridad relativas a sistemas operativos y sistemas gestores de bases de datos.
- El ITSEC (Information Technology Security Evaluation Criteria) equivalente europeo del Libro Naranja, moderno y con mayor alcance que el Libro Naranja. Se conoce como el Libro Blanco.

Con base a estos y otros estándares se construyen las políticas de seguridad para los sistemas de información.

El tema de la seguridad de la información ha tomado auge en la comunidad de habla hispana debido a que muchos de los gobiernos de la región han optado por la implementación del gobierno electrónico o gobierno en línea, como también se conoce. Motivado a esta causa muchos países han comenzado a actualizar los reglamentos jurídicos, que rigen este tipo de tecnologías de la información, actualizando a su vez las plataformas tecnológicas que soportan los sistemas de información, lo que trae como consecuencia, la verificación de la seguridad de la información de los mismos.

De igual manera la seguridad informática, de los sistemas de información es algo muy importante en Venezuela. Por lo tanto, el ordenamiento jurídico, establece reglas a seguir en diferentes aspectos relacionados con la seguridad de un Sistema de Información. La Ley Especial Contra Delitos Informáticos (2001), Ley Sobre Mensajes De Datos y Firmas Electrónicas (2001), Ley Orgánica de Telecomunicaciones (2000).

Estas normativas rigen para todos los entes organizativos del territorio venezolano. La seguridad de la información es preocupación tanto, de organizaciones públicas como privadas. Las empresas cada día necesitan del uso más inteligente de la información, para lograr ser más competitivas dentro del ambiente en que se desempeñan.

Con referencia a lo anterior, Brito y otros (2001), mencionan que en este fragmento se encuentran las Pequeñas y Medianas Empresas (Pyme's), las cuales son consideradas como un subsector productivo muy importante de la economía nacional. Ellas aportan un porcentaje importante al Producto Interno Bruto (PIB) del país.

En Venezuela las Pyme's, se definen generalmente por la cantidad de trabajadores que poseen, y la mayoría operan en el mercado regional de

cada estado al que pertenecen, convirtiéndose en generadoras de empleo, produciendo bienes y servicios que satisfacen la necesidades de la zona.

Como consecuencia de la necesidad creciente que tienen las empresas de participar y/o hacer negocios en otras regiones, de forma no tradicional (por Ejemplo: negociaciones a través de Internet), se hace necesario un análisis de sus plataformas tecnológicas, las cuales sustentan la información básica de la organización.

Por consiguiente, el uso de las Tecnologías de la Información y comunicaciones (TIC's) conlleva a analizar la seguridad informática que tienen establecida los sistemas de información empresariales. Para salvaguardar la información de dichos sistemas, se debe considerar, sí las plataformas tecnológicas están debidamente preparadas para afrontar los cambios que traen los nuevos esquemas de negocios, así como, reconocer sus debilidades y fortalezas dentro de su medio.

En ese mismo orden de ideas, se debe determinar los riesgos que podrían afectar seriamente a los sistemas de información. Ellos desempeñan un papel importante en la vida cotidiana de las organizaciones, por tanto debe asegurarse que sean exactos y confiables.

En lo referente a materia de seguridad de la información, las Pyme's presentan en la actualidad dificultades con muchos de los avances tecnológicos existentes, que podrían transformarse en riesgos potenciales. Sobre todo para el área de informática; algunas Pyme's, no están al tanto de todos aquellos recursos informáticos que podrían serle útiles para el mejoramiento operativo y estratégico de la empresa. En esta década cuando se ha afianzado el comercio electrónico y las empresas quieren, desean, y necesitan tener presencia en Internet; las Pyme's se han encontrado con una serie de factores importantes, como lo son los virus informáticos, que destruyen sus aplicaciones y/o datos; piratas de la red o hackers, que sin autorización invaden sus sistemas, sin ser detectados, para husmear, dañar o robar información. Algunas de estas empresas, participan en Internet, sin

haber evaluado previamente los riesgos a los que exponen su plataforma de información.

De lo antes expuesto, cabe mencionar, que las Pyme's, carecen del personal calificado para la administración de la plataforma informática de la empresa. Muchas veces este trabajo es realizado por los gerentes o dueños del negocio o personal adjunto al Dpto. de Contabilidad, lo que aumenta las amenazas sobre su plataforma informática.

Asimismo la mayoría de las Pyme's no poseen el capital necesario, para financiar desarrollos de sistemas de información que se amolden a sus necesidades como empresa. Muchas adquieren en el mercado de Tecnologías de la Información, sistemas transaccionales que les ayuden a solucionar la parte operativa del negocio. Pero no toman en cuenta otros elementos que son necesarios para proteger dichos sistemas.

De igual manera, la carencia de personal adecuado para el área de informática, les afecta a la hora de determinar los métodos de protección para su plataforma informática. Como que antivirus usar, con que frecuencia actualizarlos, como proteger eficientemente las redes de computadoras existentes, tanto de ataques externos, como de ataques internos; como recuperarse en caso de fallas en los sistemas de información o en caso de siniestros en las instalaciones físicas de la empresa.

Las nuevas tecnologías de información, comunicación y negocios han significado cambios paradigmáticos en la forma de pensar y de vivir de los individuos, estos cambios no son a futuro sino en el presente y sus retos emplazan a ciudadanos comunes, líderes e industriales; a que tomen decisiones bajo un clima de incertidumbre y alta movilidad organizacional.

En este sentido, es importante dar a conocer la necesidad que tiene este sector, de analizar los riesgos de seguridad informática, a los que se exponen los sistemas de información que utilizan para sus operaciones, esto con el propósito de proponer políticas de seguridad de la información que se

adapten a la pequeña y mediana empresa, con el objetivo de asegurar su plataforma informática.

Este trabajo tiene por objeto, el **"*Análisis de los Riesgos de Seguridad Informática, para las Pequeñas y Medianas Empresas (PyME's) usando el estándar ISO-17799, para la definición de políticas de seguridad que protejan sus Sistemas de Información"*.**

Para desarrollarlo se consideran las PyME's, ubicadas en la Zona industrial de Barquisimeto. Los medios para lograrlo consisten en investigación, identificación, análisis y tratamiento de los riesgos informáticos, Izquierdo (2005). Además se utiliza el estándar ISO-17799, para la formulación de políticas de seguridad de la información, por ser este uno de los más difundidos y aceptados a nivel internacional, que se refiere a la conservación e integridad de la información con la finalidad de contribuir a mejorar la seguridad de los datos de las pequeñas y medianas empresas.

De lo antes expuesto, se plantean las siguientes interrogantes:

- ¿Se pueden identificar las situaciones de riesgo que afectan la seguridad informática (física, lógica, organizacional y legal) de los sistemas de información que le sirven de apoyo a las pyme's?
- ¿Cuales son las herramientas necesarias para el control de la seguridad informática lógica, que se pueden aplicar a los sistemas de información que utilizan las pyme's?
- ¿Es necesario un conjunto de lineamientos sobre seguridad informática lógica, basados en el estándar ISO-17799 que contribuyan a mejorar el funcionamiento sus sistemas de información y se adapten a las PyME's?

Para responder a las interrogantes planteadas se formulan los siguientes objetivos:

OBJETIVOS DE LA INVESTIGACIÓN

Objetivo General:

"Analizar los Riesgos de Seguridad Informática en las Pequeñas y Medianas Empresas (PyME's), usando el Estándar ISO-17799 para la definición de políticas de seguridad que protejan sus Sistemas de Información", con la finalidad de apoyar y mejorar el desempeño de este grupo empresarial.

Objetivos Específicos:

a.- Identificar las situaciones de riesgo que afectan la seguridad informática, tomando como referencia la norma ISO-17799, en los sistemas de información que sirven de apoyo a las PyME's.

b.- Determinar las herramientas necesarias para el control de la seguridad informática, a través del análisis, categorización y monitoreo de los riesgos que afectan a los sistemas de información que apoyan a las PyME's.

c.- Proponer un conjunto de lineamientos sobre seguridad informática, basados en el estándar ISO-17799, que se adapten a las necesidades de las PyME's y que contribuyan a mejorar funcionamiento de sus sistemas de información.

JUSTIFICACIÓN E IMPORTANCIA

En la actualidad las PyME's a nivel mundial, trabajan considerablemente en establecer medidas que le permitan resguardar sus sistemas de información. Aun, muchas de ellas, no cuentan con los últimos adelantos tecnológicos en materia de seguridad para la información, además, la mayoría no tiene establecida una cultura de seguridad para los usuarios dentro de la organización o de planes de contingencia que les permitan

recuperarse rápidamente de un ataque externo o alguna problemática interna surgida en sus sistemas de información.

En tal sentido, el tema de investigación seleccionado, permitirá al investigador, mediante la aplicación de los conceptos teóricos y prácticos, sobre seguridad informática, riesgos informáticos, tecnologías de la información, presentar el desempeño de la seguridad informática en los sistemas de información que apoyan las gestiones empresariales del sector PyME's, el cual en la actualidad se encuentra afectado, por diversos cambios organizacionales tanto internos (nuevos mercados, cambios en las plataformas tecnológicas) como externos (redes ínter empresariales, comercio electrónico). Lo anterior, le facilitará al investigador establecer comparaciones entre los conceptos teóricos expuestos y la realidad encontrada en una empresa Pyme, sobre seguridad informática.

Asimismo, con este trabajo se ayudará a comprobar los niveles de seguridad informática, utilizados en las PyME's, además los resultados obtenidos se apoyaran en las normas internacionales de seguridad informática para la gestión de sistemas de información como lo son las normas ISO-17799, ampliamente conocidas y probadas en el área de seguridad de la información.

Por consiguiente, los resultados servirán de marco referencial para el establecimiento de políticas de seguridad informática en los sistemas de información de las PyME's. Igualmente, la presentación de estas propuestas, será una herramienta válida y útil, que permitirá conocer los avances de la Seguridad Informática en ésta materia y contribuir a los controles internos, proporcionando a su vez nuevos mecanismos de evaluación a los Sistemas de Información existentes.

En consecuencia, la propuesta planteada en este trabajo de analizar los riesgos de seguridad informática de los sistemas de información que se utilizan en las PyME's, favorecerá la optimización de los procesos internos, para propiciar una significativa contribución a la administración de políticas

de seguridad para los sistemas de información, y que servirá de apoyo a la gestión que realizan estas empresas.

Cabe resaltar, que el tema es de fundamental importancia para el desarrollo social y económico de este grupo empresarial. Como se menciona en el Plan Nacional de Tecnologías de la Información (2001), de Venezuela; el cual se refiere a estos nuevos cambios que enfrentan las organizaciones.

Asimismo, este estudio servirá de base para futuras investigaciones en el área de la seguridad informática, tema de amplia preocupación, dentro de la comunidad de los desarrolladores de sistemas de información del país.

ALCANCE

El estudio se propone para Analizar los Riesgos de Seguridad Informática en las Pequeñas y Medianas Empresas (PyME's), usando el Estándar ISO-17799 para la definición de políticas de seguridad que protejan sus Sistemas de Información, en la Zona Industrial de Barquisimeto. Con la finalidad de apoyar y mejorar el desempeño de este grupo empresarial en lo relacionado con sus sistemas de información.

CAPITULO II
MARCO TEÓRICO

La información se ha convertido en un activo relevante para las organizaciones, y estas se apoyan en la seguridad informática para su conservación, para lo que se utilizan diversas técnicas, normas y procedimientos. A continuación se detallan las bases teóricas que dan sustento a la investigación.

ANTECEDENTES DE LA INVESTIGACIÓN

Para la realización de este estudio se consultaron algunas Tesis de investigación relacionadas con el tema, las cuales proporcionaron información y antecedentes, a la misma.

Borghello (2001), en su tesis titulada “Seguridad Informática: sus implicancias e implementación”, describe los aspectos que puede abarcar la Seguridad informática. Este trabajo proporciona importantes definiciones sobre el tema, además de explicar todos los componentes de un sistema de seguridad informática. Concluye con los aspectos que influyen de manera contundente sobre el desempeño de la seguridad informática en la actualidad como lo son: Aislamiento y globalización, legislación vigente, tecnología existente, daños minimizables, riesgos manejables, costos, personas involucradas.

Esta tesis se relaciona con la investigación, porque el estudio proporciona información teórica, la cual es una base para el manejo e implementación de la seguridad en un sistema de información además del

establecimiento de los riesgos que podrían afectarlo, lo que favorece al logro de los objetivos de esta investigación.

Córdova (2003), en sus tesis de grado sobre “Plan de seguridad informática para una entidad financiera”, recopila información que trata lo relacionado con gestión y políticas de seguridad para la información. Entre los aspectos resaltantes menciona: usar una metodología comprobada para el diseño de un plan de seguridad de la información, el cual debe adaptarse a la empresa que lo requiera. El mismo debe incluirse en plan presupuestario de la organización, establecer los deberes y derechos de cada una de la personas que utilizan los sistemas de información, determinar qué información se protegerá y donde se encuentra; para aplicar los controles que garanticen su seguridad; el diseño de las políticas de seguridad de la información debe ser claro y jurídicamente viable, debe incluir todos los factores involucrados: tecnología, marco legal, compatible con la organización y su personal, la dirección de este plan estará a cargo de un líder organizacional, que será el encargado de la institucionalización del plan antes mencionado.

Esta tesis aporta a la investigación en estudio, conocimientos sobre las políticas o normativas que se pueden usar para el aseguramiento de la información dentro de una organización.

Mendoza (2005), trata en su Tesis “Impacto de la Tecnología de Información en la Competitividad de las Pequeñas y Medianas Industrias”, los aspectos relacionados con la implementación y aceptación de las Tecnologías de la información y comunicación, por parte de las Pequeñas y medianas industrias, donde su incorporación es lenta pero progresiva, lo que contribuye a que este tipo de empresas mejoren su grado de competitividad dentro de su entorno.

La investigación antes mencionada, aporta información sobre el uso que le da este grupo empresarial a las TIC's, las cuales motivado a los constantes cambios tecnológicos de actualidad, han tomado gran relevancia para las organizaciones que se sirven de ellas.

BASES TEÓRICAS

Las bases teóricas, permitirán aclarar los conceptos relativos al establecimiento de seguridad informática y análisis de riesgos para un sistema de información dentro de una organización.

El objetivo general de la investigación trata sobre "*Analizar los Riesgos de Seguridad Informática, para las Pequeñas y Medianas Empresas (PyME's) usando el estándar ISO-17799, para la definición de políticas de seguridad que protejan sus Sistemas de Información"*. Por lo que es necesario conocer los aspectos teóricos de este grupo empresarial.

La Pequeña y Mediana Empresa (PyME's)

A este respecto, no existe una definición clara, para este trabajo se tomará la que proporciona la Ley de Promoción y desarrollo de la Pequeña y Mediana industria (PYMI) (2001) de Venezuela en su artículo 3, que se ajusta o se aplica también a las PyME's (ver cuadro 1):

Cuadro 1. Definición de PyME's.

Tipo de Industria	Personal que Ocupa	Ventas anuales en UT
Pequeña	11 a 50	9001 a 100.000
Mediana	51 a 100	100.001 a 250.000

Fuente: Tomado y Adaptado de Berbesi (2005).

La mayoría de los países definen a la pyme por la cantidad de trabajadores que poseen o de acuerdo con el volumen de facturación anual.

Berbersi (2005) nos proporciona algunas de las ventajas y desventajas de las pequeñas y medianas empresas:

Ventajas

(1) Flexibilidad para adaptarse a los cambiantes escenarios de la economía.
(2) Aporte al empleo y al consumo.
(3) Potencial de aporte al crecimiento de la economía.

Desventajas

(1) Sistemas de gestión tradicional, desordenados.
(2) Resistentes al cambio; conservadores.
(3) Demandantes de políticas asistencialistas.
(4) Poca propensión a la asociatividad.

Las PyME's y la Tecnología:

Mora (2004), publica, sobre la asimilación de la Tecnología por parte de las PyME's, concluyendo que estas hacen poco uso de los últimos avances tecnológicos del mercado, en muchos de los casos por desconocimiento y por la falta de relación de este grupo empresarial con organismos académicos, como lo son las universidades, quienes le pueden aportar importantes avances en materia de innovación tecnológica, lo que podría beneficiar ampliamente a este sector.

En cuanto a los relacionado con las Tecnologías de la Información para las PyME's, Gaxiola (2005), publica en un articulo, sobre la trascendencia de este concepto para este grupo empresarial, señalando que con "la administración efectiva de las TIC's, se consiguen algunas ventajas: mejor manejo de los recursos tradicionales, actualización de las operaciones, reducción de tiempos, costos, aumentando los niveles de calidad y obteniendo ventajas competitivas que le permitan a las PyME's destacar". Comenta además que la mayoría de las empresas de este grupo ya poseen TIC's, pero aun no han conseguido sacarle todo el provecho, el motivo falta de alineación de los objetivos de la organización con la tecnología que estas poseen.

El autor sugiere una lista de pasos para la adopción de TIC's por parte de este grupo empresarial:

- Se debe identificar el área de la empresa. Para señalar cuales son las necesidades de información que tiene.
- Establecer los Objetivos. Por cada una de las áreas que integra una empresa, los cuales deben corresponderse con el objetivo principal de la organización.
- Deben establecerse las formas de medir los objetivos y los requerimientos de información necesarios.
- Determinar un presupuesto disponible para el proyecto.
- Proveedores de TIC ¿Comprar o desarrollar? Consultar los diferentes proveedores de servicios de TIC´s de la localidad, preguntar a otras empresas, a los empresarios del mismo ramo o de otro, en busca de opciones y posibilidades de compra de sistemas de información. Es necesario evaluar las alternativas tomando como referencia los objetivos establecidos y el presupuesto.
- Involucrar al personal. todos deben identificarse con el proceso de cambio, deben formar parte de él, conocer sus beneficios. Prepararlos con capacitación para el uso de las TIC.
- ¿Cuanto durará el Proyecto? Determinar el tiempo adecuado para la puesta en funcionamiento de los nuevos recursos en tecnologías de la información. Crear un plan de trabajo claro y preciso.

Ledón (2005), agrega que "actualmente la tecnología ha resultado ser vital para las PyME's, debe ser una herramienta integrada en los procesos de estas organizaciones. Es un catalizador de innovación y transformación en las empresas".

De lo antes expuesto, se puede concluir que las empresas tipo PyME, necesitan de alguien que las guíe u oriente en la adquisición de TIC's, las cuales podrían resultar ampliamente beneficiosas, si son administradas de forma oportuna, responsable y eficiente, con el fin de aprovechar las ventajas competitivas que estas les ofrecen.

Otro factor que afecta el desarrollo de la PyME, es el relativo a las personas, o capital humano como también se le conoce.

Las PyME's y Recursos Humanos

Mora (2004), explica que el factor de "recursos humanos no se ha sabido valorar por parte de las PyME´s, debido a la poca capacitación, desarrollo deficiente de este recurso, baja motivación organizacional, alta rotación, lo que redunda en poca productividad empresarial". Además, otra limitante es que las PyME's no logran valorar el recurso humano, en muchos casos por desconocimiento o por falta de interés por parte de la directiva de la organización, la cual no incluye, este importante recurso dentro sus estrategias de negocio. Es muy importante que una empresa involucre en su proceso de desarrollo los recursos materiales y recursos humanos.

Siguiendo con el objetivo general de la investigación, a continuación se presentarán las bases teóricas relacionadas con la seguridad de la información y sus riesgos.

Seguridad informática o Seguridad de la Información:

Espiñeira, Sheldon y Asociados (2005), comentan en su publicación, una definición de Seguridad de la Información o Seguridad informática, como también se le conoce, refiriéndola como la "encargada de proteger los activos de información de una organización contra pérdidas o el uso indebido de la misma, además de permitir el acceso a los activos de la información, dando apoyo a los objetivos de la organización". Cabe agregar que la misma cumple un rol estratégico en los procesos de negocios identificando los recursos que deben resguardarse o restringirse dentro una empresa, lo cual conlleva a mejorar las operaciones con clientes, socios, proveedores y empleados. En el gráfico siguiente (ver figura 1), se muestra la relación de la seguridad de la información con los recursos organizacionales.

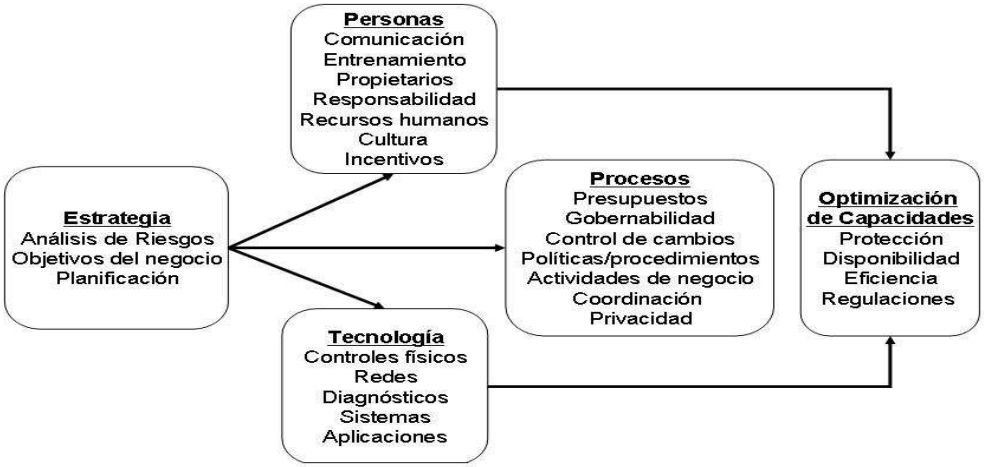

Figura 1.
Fuente: Tomado y adaptado de Espiñeira, Sheldon y Asociados (2005), Seguridad de la Información: Componente Organizacional, Recursos, Procesos y Tecnología.

De estas consideraciones se desprende, que el concepto de seguridad informática, no es sólo un aspecto tecnológico, es también es una solución integrada de negocio que combina los recursos organizacionales, procesos y tecnología. Por lo que se debe contar con reglas, lineamientos, asignación de responsabilidades, además de incluir los procedimientos preestablecidos, y personal capacitado para la gestión del proceso.

Bossio y Gros (2003), exponen que el término de la seguridad informática para sistemas de información, no es algo nuevo, existe desde hace tiempo, solo que ahora se encuentra en fase de evolución permanente debido a los avances técnicos en materia informática. Los autores expresan que los avances de la actualidad, en el que se destaca, el auge de la globalización y la apertura de las telecomunicaciones; los riesgos y las amenazas aumentan en forma alarmante.

En este orden de ideas, la seguridad informática o de la información se basa en tres pilares fundamentales, como son:

Confidencialidad: es el aseguramiento de que la información, no es accesada por personas o entidades no autorizadas.

Integridad: garantiza que la información es creada, modificada o eliminada solo por el personal autorizado.

Disponibilidad: los datos o la información estarán al momento y en la forma en la son requeridos por el personal autorizado.

Asimismo, en la actualidad debido a los avances tecnológicos, se habla de otro principio que tiene relación con la aceptación/no aceptación, o repudio o no repudio, como lo mencionan algunos autores. Este se basa en la aceptación de un mensaje y en la constancia de envío del mismo. El proceso es realizado a través del seguimiento electrónico del mensaje y la utilización de los certificados digitales o firmas digitales. De esta forma se asegura que todo mensaje tenga un destino y un origen de forma fiable, que se puede determinar mediante procesos de auditoria informática.

Además de los pilares antes mencionados, el objetivo principal de la seguridad informática es la preservación y adecuada distribución de la información, pero de este se derivan otros objetivos secundarios.

Oz (2002), recopila, algunos de estos objetivos, los cuales se detallan a continuación:

- Reducir el riesgo de que los sistemas de información y de que las organizaciones, cesen sus operaciones.
- Mantener la confidencialidad de la información.
- Asegurar la integridad y confiabilidad de los datos.
- Asegurar la disponibilidad de los datos o la información.
- Asegurar el cumplimiento de las leyes de seguridad nacionales para seguridad de la información, las de los directivos y las reglas de privacía.

Así como es ventajoso para una organización gestionar eficientemente su seguridad de la información, no se puede dejar de mencionar que este proceso también puede generar algunas desventajas como las que se mencionan a continuación:

Desventajas de la Seguridad Informática

Laudon (2002), menciona algunos argumentos que podrían presentarse al momento de establecer políticas o procedimientos para la seguridad de la información o planes de seguridad informática. Explica que "la construcción de los mecanismos de control para un sistema de información pueden ser muy costosos y complicados para su empleo, lo que no es económico y tampoco operativamente factible". Es preciso que la organización analice la relación costo/beneficio y determine los mecanismos de control que le ofrezcan la protección más eficiente, sin necesidad de reducir eficiencia operativa e incrementar gastos en el presupuesto.

Oz (2002), complementa estas desventajas, agregando las siguientes:

- Comunicaciones más lentas (por el uso de algoritmos de Encriptación de datos, uso de Firewalls para las redes de telecomunicaciones).
- Molestia de los empleados, por nueva normativa para el uso de los sistemas de información, acceso al hardware, al software, a las aplicaciones (uso restringido de Internet), ingreso a las instalaciones de la organización.
- Olvido de contraseñas, debido a la frecuencia de cambios. Planes de entrenamiento para la explicación de las nuevas políticas de seguridad de la empresa.

En relación al establecimiento de la seguridad de la información existen una serie de creencias que podrían afectarla. Jiménez (2005), reseña un listado de paradigmas organizacionales relativos al tema:

- Generalmente existe la creencia de que los procedimientos de auditoria son responsabilidad del personal del centro de cómputo, pero se debe cambiar este paradigma y dar a conocer que estas son responsabilidades del usuario y del departamento de auditoria interna.
- Muchas compañías cuentan con dispositivos de seguridad física para los computadores y se cree que los sistemas no pueden ser violados si no se ingresa al centro de cómputo, no se

tienen en cuenta el uso de terminales y de sistemas para el acceso remoto.

- Otra creencia es que los casos de inseguridad que tratan de sistemas de seguridad contra incendio o robo, son innecesarios; "eso no puede suceder aquí" o “es poco probable que suceda".
- Pensar que los computadores y los programas son tan complejos que nadie fuera de la organización los va a entender y no les van a servir, ignorando a las personas que puedan captar y usarlos para otros fines.
- Los sistemas de seguridad generalmente no consideran la posibilidad de fraude interno, que generalmente es realizado por el mismo personal en el desarrollo de sus funciones.
- Creer que la seguridad por clave de acceso es inviolable, pero no se considera a los delincuentes sofisticados con tecnología avanzada.
- Suponer que los defectos y errores son inevitables.
- Creer que se hallan fallas porque nada es perfecto.
- Creencia de que la seguridad se aumenta solo con la inspección.

En la lista se refieren los más comunes, pero sin embargo, no son todos. Cada gerente o propietario de empresa tiene los suyos, sin excluir a los del personal responsable de la informática dentro de la organización. Por ende es necesario de que exista una fluida y clara comunicación entre la alta gerencia de una empresa y el área de informática, que permite la alineación de las estrategias de negocio con relación al tema de la seguridad de la información.

Además, de las desventajas y paradigmas organizacionales, se debe agregar algunos nuevos elementos incorporados a la sociedad de la información, como pueden ser: la ética, el surgimiento de nuevas figuras digitales y la inmaterialidad de la información, la falta de cultura digital en las sociedades actuales, como lo refieren, Lizama y Farias (2003).

Continuando con las aclaraciones sobre el término de seguridad informática, es necesario mencionar los tipos más conocidos:

Tipos de Seguridad informática:

Seguridad Informática Física:

Ramió (2006), menciona que la Seguridad Física, “puede asociarse a la protección de los sistemas ante las amenazas físicas, incendios, inundaciones, edificios, cables, control de accesos de personas, etc.” Esta se encuentra estrechamente relacionada con todos los soportes físicos que utilizan los sistemas de informática para el manejo de la información, lo que incluye al hardware, componentes para redes de telecomunicaciones, todas las instalaciones donde se encuentran los equipos, dispositivos para la electricidad, etc. El objetivo de este tipo de seguridad es asegurar la plataforma básica donde circula la información.

Seguridad Informática Lógica:

Este tipo de seguridad informática, se encuentra ligada a todo lo que tiene que ver con software y los elementos necesarios para emplear la información.

Con relación a lo anterior, Donado y otros (2002), proporcionan una definición de seguridad informática lógica, en la que se refiere como “todos los recursos de computación lógicos como: sistemas operativos, bases de datos, programas de desarrollo, editores, etc. Los cuales intervienen en el manejo de la información, incluye además los procedimientos y la administración de los programas”.

Ellos explican algunos de los objetivos de la seguridad lógica que se desglosan a continuación:

- Información disponible: indica que el usuario debe tenerla siempre que la requiera.

- Confidencialidad de la información: se relaciona con la autorización del usuario para el acceso a la información.
- Integridad de la información: solo el personal autorizado puede modificar la información.
- Consistencia del sistema: los sistemas deben funcionar para lo que fueron programados, cumpliendo los objetivos y procedimientos asignados, cualquier modificación estará a cargo del personal autorizado.
- Control de acceso a los sistemas: debe ser posible rastrear o monitorear el acceso de los usuarios a los sistemas, por medio de procedimientos o herramientas especializadas.
- Auditoria de programas: el administrador de los sistemas debe conocer las tareas que realizan los usuarios durante los accesos a los mismos.

Seguridad organizacional administrativa:

Procura cubrir el vacío, dejado por las dos anteriores, y trata en cierto modo de complementarlas. Es difícil, lograr de forma eficaz la seguridad de la información, si no están claramente definidas:

- Políticas de seguridad.
- Políticas de personal.
- Políticas para el Análisis de riesgos.
- Planes de Contingencia en caso de fallas.

Tareas que son responsabilidad de la alta gerencia de una organización, además son los directivos los que deben decidir que se debe proteger, a que costo y quienes son los encargados de brindar esa protección a la información de la organización.

Seguridad jurídica o Legal:

Su objetivo es lograr a través de la aprobación de normas legales o reglamentos, el marco jurídico necesario para proteger los bienes informáticos y la información que se genera a través de estos. Esta a cargo de los organismos legislativos de cada país, que tienen el deber y el derecho de reglamentar, todo lo relacionado con los activos informáticos tanto de las organizaciones públicas, como de las privadas.

Tomando como base la clasificación anterior, se hace necesario el establecimiento de normas, procedimientos y técnicas que permitan la administración eficiente de la seguridad de la información, tarea principal que cumple la gestión de la seguridad informática.

Gestión de la seguridad de la Información

Villalón (2005), destaca que la gestión de la seguridad "consiste en la realización de las tareas necesarias para garantizar los niveles de seguridad exigibles en una organización. Además agrega que la seguridad es un proceso, no un producto y hace referencia al modelo PDCA: Planificar, Hacer, Verificar y Actuar", el que se muestra a continuación (ver figura 2) y donde se aprecia el ciclo de calidad que debe seguir, la gestión de la seguridad informática:

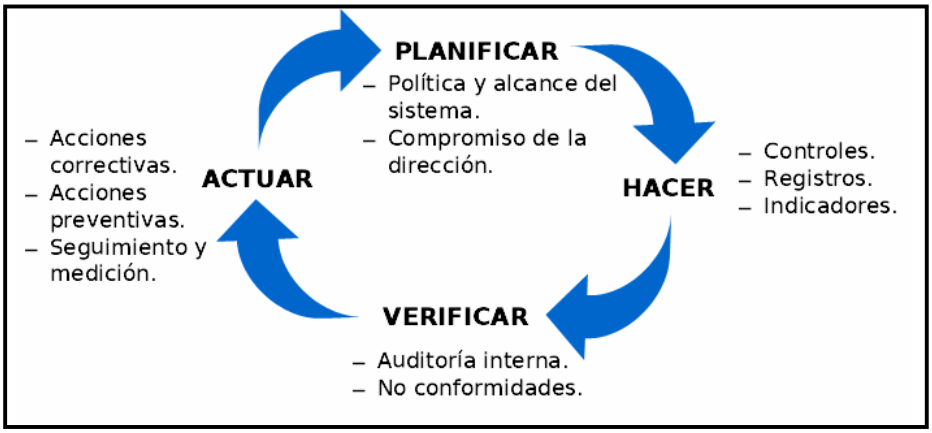

Figura 2.
Fuente: Villalón (2005). Modelo PDCA, Calidad de la seguridad**.**

Villalón, (2005), menciona que "la organización debe converger hacia un sistema de gestión único, capaz de agrupar Calidad, Medioambiente, Seguridad de la Información, etc.". Lo que indica que no todos los problemas que surjan con la seguridad informática, estarán relacionados con la tecnología que la sustenta.

De igual manera, O'Brien (2001), describe los controles que se requieren para el establecimiento de seguridad en un sistema de información, los cuales buscan garantizar la exactitud, integridad y protección de los recursos y actividades del sistema de información y los agrupa en tres categorías:

- Controles de los sistemas de información: metodologías y dispositivos para garantizar la exactitud, validez e idoneidad de las actividades del sistema. Verifican el ingreso de datos, las técnicas para procesarlos, el almacenamiento y la salida de los mismos.
- Controles de procedimientos: se establecen para indicar como deben operarse los recursos computacionales y de red, dentro de la organización, garantizan la exactitud e integridad de las operaciones.
- Controles de instalaciones: métodos para proteger contra perdida o destrucción, las instalaciones de redes y computadoras dentro de una organización. Es necesario contar diversos dispositivos de seguridad y procedimientos para proteger los recursos de hardware, software, redes de comunicaciones y datos de una empresa.

Dentro de la gestión de la seguridad de la información, las políticas ocupan un espacio muy importante, debido a que no se puede establecer seguridad informática confiable, sin un conjunto de políticas que la respalden dentro de la organización.

Políticas de Seguridad informática o de la información:

Torres (2003), describe la importancia de definir políticas para la seguridad informática. Aduce que estas:

> Deben ser definidas e implantadas por la alta gerencia de la empresa y deben difundirse a todo el personal de la organización. Estas políticas de seguridad informática proporcionan delimitaciones claras que definen un dominio donde se puede encontrar una solución aceptable, cuando surja algún problema que afecte la seguridad de la información.

Indica además que dichas políticas representan un tipo especial de reglas de negocio documentadas. De esta forma los que trabajan en el ambiente empresarial podrán recibir instrucciones claras y definitivas que los ayuden a establecer la seguridad de la información generada en el complejo mundo de los negocios. Es la gerencia la que debe involucrarse en la seguridad informática, asignar los recursos y comunicar clara y oportunamente, a todos los integrantes de su equipo que la seguridad informática es importante para su empresa, este factor es clave para la implantación de políticas de seguridad de la información exitosas.

El autor conceptualiza las políticas como “requisitos generalizados que deben ser escritos en papel y comunicados a ciertos grupos de personas dentro y cuando se requiera, fuera de la organización. Estas funcionan como reglas de negocios”. Los documentos de políticas de seguridad informática varían de una organización a otra, un documento de este tipo incluye los argumentos o razones de las políticas, la descripción de las personas a quienes va dirigidas, el historial de las modificaciones efectuadas, definiciones de términos especiales y las instrucciones gerenciales específicas sobre el tratamiento que se le dará a las políticas. Tienen carácter obligatorio y pueden considerarse el equivalente de una ley propia para la organización que las aplique.

Por otra parte, la gerencia de toda organización, debe establecer sus objetivos con respecto a la operación de los computadores, aplicaciones, bases de datos y las redes de telecomunicaciones, por lo que debe dedicar tiempo a preparar una política de seguridad informática y su correspondiente documentación. Las políticas además representan para la gerencia una manera relativamente económica y directa de definir el comportamiento en relación con la seguridad informática.

Witte (2003), define política de seguridad como: “Conjunto de Normas y Procedimientos documentados y comunicados, que tienen por objetivo minimizar los riesgos informáticos más probables y reglamentar el uso de los

componentes de un sistema de información". Además el autor menciona los elementos involucrados en estas políticas como "las herramientas usadas para el establecimiento de la seguridad de la información y el cumplimiento de las tareas por parte de las personas involucradas".

En relación a esto último, la empresa consultora ITELLIGENCE de Venezuela (2005), ofrece una lista de consideraciones importantes sobre el tema:

- Mostrar a la gerencia los verdaderos requerimientos de seguridad de la información.
- Cultura organizacional. Enfocar la atención del trabajador en lo esencial. Evitar disputas internas. Coordinar las actividades para mantener la seguridad de forma continua.
- Definir los límites de las acciones que se pueden permitir.
- Controlar con anticipación los eventos relativos a la seguridad.
- Coordinar actividades de grupos internos y externos (relación con otras organizaciones).
- Reducir los costos mediante la normalización de los controles.
- Cumplir las obligaciones contractuales y responsabilidades legales.

La firma consultora agrega además, los factores críticos para el éxito de la implantación de políticas sobre seguridad informática en una organización:

- Gestionar los riesgos, cubriendo todos los componentes internos y externos, la naturaleza de los sistemas, las actividades empresariales y las leyes locales.
- Identificar todos los terceros involucrados (Clientes / Usuarios / Proveedores / Socios de negocio / Otras Organizaciones / Gobierno).
- Identificar e inventariar todos los activos informáticos.
- Las políticas deben estar desarrolladas de acuerdo con los objetivos del negocio y adaptadas a la cultura organizacional.
- Deben contar con el apoyo y compromiso manifiestos por parte de la gerencia.
- Participación de todo el personal involucrado a través de equipos multidisciplinarios.
- Claro entendimiento de los requerimientos de seguridad.
- Sistema de medición para evaluar el desempeño de la gestión de la seguridad.
- Asignación y disponibilidad de recursos.

En el gráfico siguiente (ver figura 3), se describe el ciclo necesario para la creación de políticas de seguridad informática y su administración, en una organización.

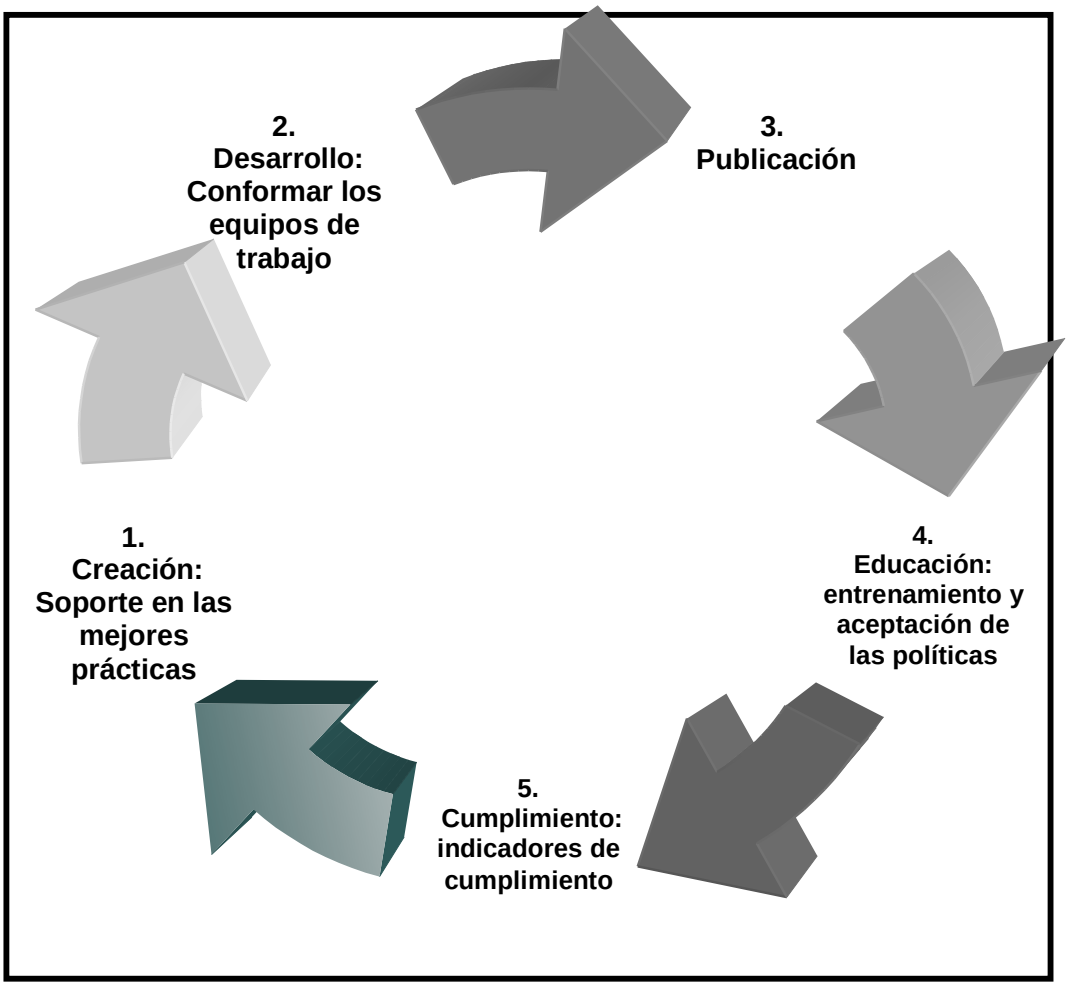

Figura 3.
Fuente: tomado y adaptado ITELLIGENCE de Venezuela (2005), Ciclo de Administración de las políticas de Seguridad.

Villalón (2005), resume de forma objetiva la función principal de la implantación de políticas de seguridad para la información:

Cuadro 2. Implantación de políticas de seguridad.

Política de Seguridad (adaptadas a las necesidades de la organización y documentadas)
⇩
Normativas (creadas por la alta gerencia)
⇩
Implantación (dentro de la Organización)
⇩
Mecanismos de seguridad (prevención, detección, Recuperación)

Fuente: tomado y adaptado. Villalón (2005).

El esquema describe como debe ser el proceso de adopción de políticas de seguridad por parte de una organización. Señalando como primer paso crear o diseñar las políticas ajustadas a las necesidades empresariales para la protección de su información, las mismas se apoyan en un conjunto de normativas que serán aplicadas por áreas especificas y estas normativas servirán de base para la implantación de los mecanismos de seguridad necesarios para dar cumplimiento a las políticas establecidas.

Barzanallana (2006), menciona algunas de las medidas de seguridad que se pueden establecer, para lograr el aseguramiento de la información, como se muestra en la tabla a continuación (ver figura 4 y cuadro 3):

Tipos	Protección Física	Medidas Técnicas	Medidas de Organización
Preventivas	PF	PT	PO
Detectivas	DF	DT	DO
Correctivas	CF	CT	CO

Figura 4
Fuente: Barzanallana (2006), Medidas de Seguridad

Cuadro 3. Medidas de Seguridad.

PF: vigilantes a la entrada del edificio, control en el acceso, protección al hardware, respaldo de datos.	**DT:** control de acceso lógico, sesión de autenticación
	CT: programa antivirus
DF: monitor de vigilancia, detector de metales, detector de movimiento.	**PO:** cursos de actualización, organización de las claves.
CF: respaldo de alimentación eléctrica	**DO:** monitoreo de auditoria
PT: firewalls, criptografía, bitácora	**CO:** respaldos automáticos, plan de incidentes (sanciones)

Fuente: Barzanallana (2006).

Para concluir, es necesario comprender que las medidas o procedimientos de seguridad para la información por si solos no bastan, es necesario realizar una planificación adecuada que cumpla con los objetivos del negocio, para asegurar una gestión apropiada de la seguridad informática.

Además del establecimiento de políticas de seguridad informática, una gestión de seguridad informática eficiente, tendrá en cuenta todos los riesgos que puedan afectar leve, moderada o gravemente a los sistemas de información de una organización.

Riesgos o vulnerabilidades de la Seguridad de la información

En todo plan para la gestión de la seguridad de la información, es necesario, estudiar y clarificar los riesgos empezando por determinar que se protegerá, de que se protegerá y como se hará. Este proceso permite analizar todos los riesgos y establecer prioridades de acuerdo con su complejidad. Además se deben examinar los costos de proteger y la tasa de

retorno, estableciendo proporciones de acuerdo con lo que se desea proteger.

Continuando con la descripción del tema, es necesario conocer los términos que se relacionan estrechamente con el análisis de riesgos:

- Activo: es un recurso del sistema de información o que se relaciona con éste, y es necesario para que la organización funcione correctamente y alcance los objetivos propuestos.
- Amenaza: un evento que puede desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos de la información.
- Impacto: consecuencia producida por la realización de una amenaza.
- Riesgo: es una posibilidad de que se produzca un Impacto determinado en un Activo, en un Dominio o en toda la Organización.
- Vulnerabilidad: es la posibilidad de ocurrencia de la materialización de una amenaza sobre un Activo.
- Ataque: evento, exitoso o no, que atenta contra el buen funcionamiento del sistema.

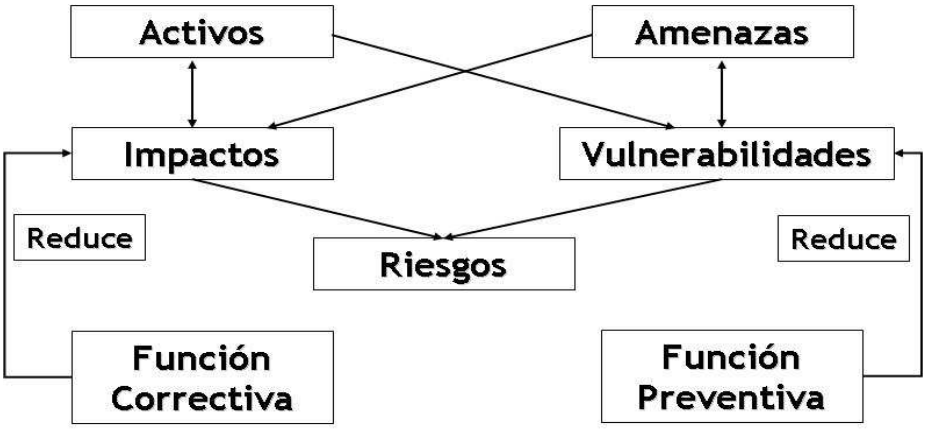

Figura 5.
Fuente: Witte (2003), Análisis de riesgos, modelo de gestión.

El gráfico anterior (ver figura 5), muestra la relación entre corregir y prevenir, para lograr una gestión de riesgos exitosa.

Sena y Tenzer (2004), definen los riesgos como: “eventualidades que imposibilitan el logro de un objetivo”, lo cual puede derivar en perdidas para la organización.

Izquierdo (2005), agrega que el riesgo, “es una probabilidad de que una amenaza explote vulnerabilidades de un activo o conjunto de activos y cause perdida o daño a los mismos”.

Por otra parte la ISO, define al riesgo tecnológico como: “Probabilidad de que una amenaza se materialice, usando las vulnerabilidades existentes de un activo o un grupo de ellos, generando perdidas o daños”.

Asimismo, Villalón (2005) expresa que a las “medidas que eliminen la vulnerabilidad o la amenaza, o disminuyan el riesgo o impacto asociados, se les denomina defensas, salvaguardas o controles”.

De lo antes expuesto, se desprende que la determinación de los riesgos dentro de los ambientes informáticos es importante para una organización, porque le ayuda a prevenir futuros inconvenientes, relacionados con las tecnologías de la información que se tengan en funcionamiento, además de establecer las políticas necesarias para la administración eficiente de los riesgos, lo que redundará en planes de contingencia oportunos, en el caso de que se presentasen riesgos o amenazas comprometedoras, así como, determinación de las medidas preventivas para el uso de los recursos tecnológicos disponibles dentro y fuera de la organización.

A este respecto, el proceso de administración de riesgos consiste en determinar las posibles causas o problemas que se pueden presentar en una empresa y que afecten a los sistemas informáticos, y de cómo deben tratarse las situaciones cuando estas se presenten, de forma tal que los activos de la información disminuyan su vulnerabilidad a sufrir un ataque o impacto, o en el mejor de los casos gestionar los riesgos que surjan.

En este propósito, uno de los primeros pasos en la administración de riesgos para sistemas informáticos, es realizar una evaluación de las vulnerabilidades o riesgos de dichos sistemas, para determinar los puntos débiles que afectan seriamente las operaciones del negocio en relación con las TIC's que utilizan. Algunos de los elementos a verificar: configuración de los dispositivos de red como Switches, Routers, Firewalls, IDS, Servidores de datos, de comunicaciones, conexiones móviles o remotas (Internet, laptops, palm, tele trabajo, etc.), verificación de la seguridad de los sistemas operativos (actualización de parches), antivirus y sus actualizaciones respectivas, privilegios acceso a las bases de datos, unidades de backups o respaldos de información, frecuencia de backups, entre otros.

La información del análisis puede presentarse como un informe que ayude al personal encargado de los sistemas informáticos, a determinar los posibles impactos que podrían sufrir en algún momento estos sistemas y lo cual podría afectar el desempeño de las operaciones en la organización.

Izquierdo (2005), aclara los beneficios que le proporciona a la organización una adecuada administración de riesgos:

- Mejora el logro de los objetivos organizacionales.
- Ayuda a la organización a estar más segura y consciente de sus riesgos.
- Desarrolla el control interno.
- Optimiza la asignación de recursos.
- Aprovechamiento de oportunidades de negocio.
- Fomenta la cultura del autocontrol.
- Estabilidad ante cambios del entorno de la organización.

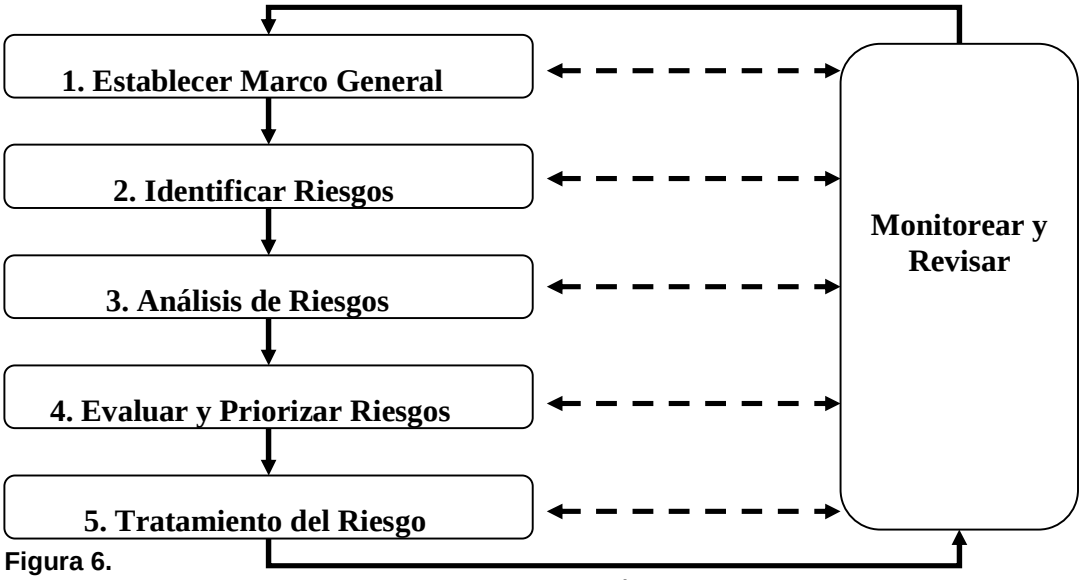

Figura 6.
Fuente: Izquierdo (2005), Proceso de la Administración de Riesgos

En el gráfico anterior (ver figura 6) se muestra un esquema del proceso de administración de riesgos, identificando cada una de las etapas que involucra este proceso, además incluye una fase de monitoreo y revisión continua, lo que conlleva a mejorar la retroalimentación de la administración de riesgos.

En la actualidad existen algunas herramientas que pueden ayudar a los especialistas a determinar y medir los riesgos de una organización. Una de estas herramientas es el Sistema MAGERIT.

MAGERIT, significa "Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas". Es una metodología de carácter público, perteneciente al Ministerio de Administraciones Públicas de España. Es un método formal para investigar los riesgos que soportan los sistemas de información, y para recomendar las

medidas apropiadas que deberían adoptarse para controlar estos riesgos. Este sistema fue elaborado por un equipo multidisciplinario del Comité Técnico de Seguridad de los Sistemas de Información y Tratamiento Automatizado de Datos Personales, SSITAD, del Consejo Superior de Informática. A continuación se presenta un gráfico (ver figura 7) que muestra la estructura funcional de dicho sistema.

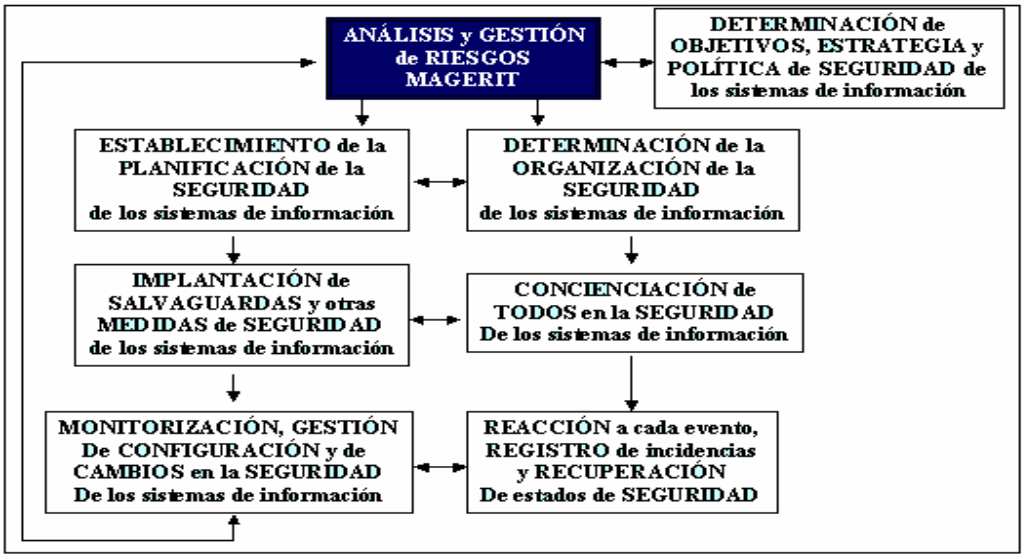

Figura 7.
Fuente: Consejo Superior de Informática, Ministerio de Administraciones Públicas, España. Funcionamiento de Magerit.

De lo anteriormente expuesto, hay que agregar que otra de las tareas del análisis de riesgos, es la de determinar y prevenir las amenazas hacia los sistemas informáticos organizativos.

Amenazas

Entre los objetivos de la seguridad de la información, está la de protegerla, tanto de amenazas fortuitas, como deliberadas. Ellas, afectan principalmente al hardware, al software y a los datos.

Bossio y Gros (2003), listan algunas de las posibles amenazas a las que se enfrenta una organización en la actualidad:

- La mayor parte de los fraudes ocurren a través del uso de los sistemas.
- Una empresa puede ser enjuiciada por incumplimiento de leyes y reglamentaciones (Habeas Data, (propiedad Intelectual). legalidad)
- En los equipos puede haber software no licenciado (pirata).
- La propiedad de la información y el desarrollo a favor de la empresa puede no estar asegurada (falta de contratos).
- Algunos empleados y terceros pueden no conservar o respetar los contratos de confidencialidad.
- Confidencialidad relacionada con:
  - Distribuir información.
  - Distribuir datos que atenten contra la privacidad de los empleados.
  - Obtener la documentación impresa de la basura.
  - Acceso a la información no recogida de las impresoras por parte de personas ajenas a la organización.
- Disponibilidad: Se puede no disponer de la información en el momento adecuado.

Witte (2003), complementa la lista anterior agregando las siguientes variables:

- Accidentes: Averías, Catástrofes, Interrupciones.
- Errores: de Uso, Diseño, Control.
- Intencionales Presénciales: Atentado con acceso físico no autorizado.
- Intencionales Remotas: Requieren acceso al canal de comunicación. Dentro de las cuales se encuentran:
- Interceptación pasiva de la información (amenaza a la confidencialidad).
- Corrupción o destrucción de la información (amenaza a la integridad).
- Suplantación de origen (amenaza a la autenticación).

Por otra parte, Witte (2003), relaciona algunas de las causas que han aumentado las amenazas para la seguridad de la información:

- Crecimiento exponencial de las redes y de los usuarios Interconectados.

- Aumento de las Bases de Datos On-Line.
- Inmadurez o mal manejo de las Nuevas Tecnologías de la información.
- Amplias herramientas automatizadas especializadas en ataques informáticos.
- Nuevas técnicas de ataque distribuido.
- Técnicas de Ingeniería Social para capturar las identificaciones de usuarios válidos).

Entre los aspectos más relevantes para la seguridad informática, se encuentra la gerencia conveniente de la misma, dado que existe mucha tecnología aplicable para la protección de uno de los principales activos de la organización, como lo es la información, pero sin la colaboración y el establecimiento de políticas adecuadas por parte de las directivas de la empresa, que permitan gestionar eficientemente dicha seguridad informática, el progreso es lento y los resultados impredecibles.

Continuando con algunas de las tareas de la gestión de riesgos informáticos, se incluye el apartado de los ataques informáticos, los cuales en la actualidad resultan agresivos y dañinos hacia un sistema informático.

Ataques informáticos

Al momento de establecer políticas de seguridad para la información, es necesario determinar que tipos de ataques informáticos podrían afectar a dicho sistema. Hoy día con los avances tecnológicos del momento, cualquier organización puede ser victima de un ataque informático en sus sistemas. Partiendo de la premisa de que “la seguridad total no existe”, es un indicativo de que se deben conocer los ataques o amenazas que pueden afectar una empresa.

Ramió (2006), nombra algunos de estos ataques para un sistema informático (ver cuadro 4):

Cuadro 4. Ataques a sistemas informáticos.

❖ Fraude	❖ Malversación	↳ Robo
❖ Sabotaje	❖ Espionaje	↳ Chantaje
❖ Revelación	❖ Virus	↳ Mascarada
❖ Gusanos	❖ Caballos de Troya	↳ Spam

Fuente: tomado y adaptado. Ramió (2006).

Agrega además, que en el año 2005, aparecen nuevas formas de ataque como son: Ingeniería social, phishing, Spyware, entre otros. A continuación se citan algunos de los más importantes:

Virus de Computadora: definidos como código de programación, generalmente de reducido tamaño, que insertado dentro de un programa modifica o destruye datos. Tienen la propiedad de reproducirse o copiarse a otros programas, propagando la infección o los daños.

Personas:

Generalmente relacionadas con el área de informática, pueden ser desarrollares o programadores de software, expertos en redes o telecomunicaciones, en resumen personas que aprovechan todos sus conocimientos académicos y técnicos para infringir, causar daños intencionales o no, cometer actividades delictivas, hacia la información o datos de una organización.

Ramió (2006), proporciona algunas definiciones sobre los términos relacionados con los piratas de la informática, como se les conoce en el argot popular de la informática:

- Hacker: Definición inicial de los ingenieros, que hacían alardes de sus conocimientos en informática. Entre muchas clasificaciones están las de White Hat (generalmente no delictivos), Black Hat (generalmente es delictivo) y Grey Hat (reconvertidos por la empresa).

- Cracker: Persona que intenta de forma ilegal romper la seguridad de un sistema por diversión o interés.
- Script kiddie: Un inexperto, normalmente un adolescente, que usará programas que se descarga de Internet para atacar sistemas.

Ante esta situación, el proceso de globalización, ha traído consigo nuevas formas de ataque hacia los sistemas informáticos, lo cual indica que las empresas deben estar concientes de que su participación dentro de Internet, debe estar planificada, controlada y supervisada por personal calificado, que le permita reaccionar con prontitud ante cualquier amenaza o ataque. Las organizaciones con presencia en Internet deben contar con las herramientas necesarias para proteger la seguridad de sus sistemas.

Por otra parte, el negocio de la información, se ha convertido en algo atractivo para los delincuentes informáticos, quienes tienen los conocimientos, las herramientas y el tiempo necesario para dedicarse a burlar cualquier sistema de seguridad. Queda por parte de las empresas u organizaciones establecer los mecanismos de control que le permitan detectar, controlar y/o evitar cualquiera de los ataques de los que sea objetivo.

De igual manera, es importante conocer el estándar más usado a nivel internacional para la seguridad de la información, el cual fue creado con el objetivo de fundamentar normas o políticas para la conservación de la información dentro de un sistema informático.

Estándar Internacional para la Seguridad de la Información ISO-17799

Normas ISO-17799

El portal de las norma ISO en español (Internet), describe el funcionamiento y aplicabilidad de esta norma. La ISO (International Organization for Standardization) es la Organización Internacional para la Estandarización, nacida en Febrero de 1947 y radicada en Ginebra, cuenta

con la representación de 153 países, y tiene como objetivo lograr la coordinación internacional y la unificación de estándares para la industria.

El ISO 17799, se define como una guía en la implementación del sistema de administración de la seguridad de la información, dirigido a preservar los siguientes principios de la seguridad informática:

Confidencialidad. Asegurar que únicamente personal autorizado tenga acceso a la información.

Integridad. Garantizar que la información no será alterada, eliminada o destruida por entidades no autorizadas.

Disponibilidad. Asegurar que los usuarios autorizados tendrán acceso a la información cuando la requieran.

El estándar, para la administración de la seguridad de la información, fue publicado por la ISO en diciembre del 2000 con el propósito de desarrollar un marco de seguridad sobre el cual trabajen las organizaciones. El objetivo de la seguridad de los datos es garantizar la continuidad de las operaciones de la organización, reduciendo al mínimo los daños causados por una contingencia, logrando así optimizar la inversión en tecnologías de seguridad de la información.

Los principios de la norma para la protección de los activos de información, constituyen las reglas básicas para cualquier organización, sean instituciones de gobierno, educativas o de investigación, sin embargo, depende de la naturaleza y las metas de las organizaciones. Este estándar define, cuáles metodologías, normas o estándares técnicos pueden aplicarse al sistema de administración de la seguridad de la información. La aplicación de un marco de referencia de seguridad basado en el ISO 17799, proporciona beneficios a toda organización que lo implemente, al garantizar la existencia de una serie de procesos que permiten evaluar, mantener y administrar la seguridad de la información. Lo que resulta muy importante en aquellos convenios o contratos con terceras organizaciones que establecen como requisito el uso de la norma.

El ISO 17799, se deriva de la norma BS7799 de BSI (British Standards Institution) que aparece por primera vez en 1995, con objeto de preparar a cualquier empresa británica o no en la certificación de la gestión de la seguridad de su información por medio de una auditoria realizada por un auditor acreditado y externo a la empresa. El gobierno del Reino Unido recomendó como parte de su Ley de Protección de la Información que las compañías británicas emplearan el estándar BS7799, como método de cumplimiento de la Ley.

La primera parte de la norma (BS7799-1) es una guía de buenas prácticas, para la que no se establece un modelo de certificación. Es la segunda parte (BS7799-2) la que permite auditar y certificar, a las empresas solicitantes que hayan desarrollado un SGSI (Sistema de Gestión de Seguridad de la Información) según el modelo PDCA (acrónimo inglés: Plan-Do-Check-Act; Planificar-Hacer-Verificar-Actuar), implementado en otros estándares como el ISO 9000, y que asegura la adaptación continua de la seguridad a los requisitos siempre cambiantes de la empresa y su entorno.

Las dos partes de la norma BS7799 se revisaron en 1999 y la primera parte se adopta por ISO, sin cambios trascendentes, como ISO17799, en el año 2000, con una aceptación de más de ochenta mil empresas. En el 2005, el esquema SGSI de la norma se publica por ISO bajo la norma 27001, junto a la primera revisión formal realizada en ese mismo año de ISO 17799, basándose principalmente en la 1era parte del estándar BS 7799, conocido como código de buenas prácticas. En el siguiente gráfico se muestra la evolución del estándar (ver figura 8):

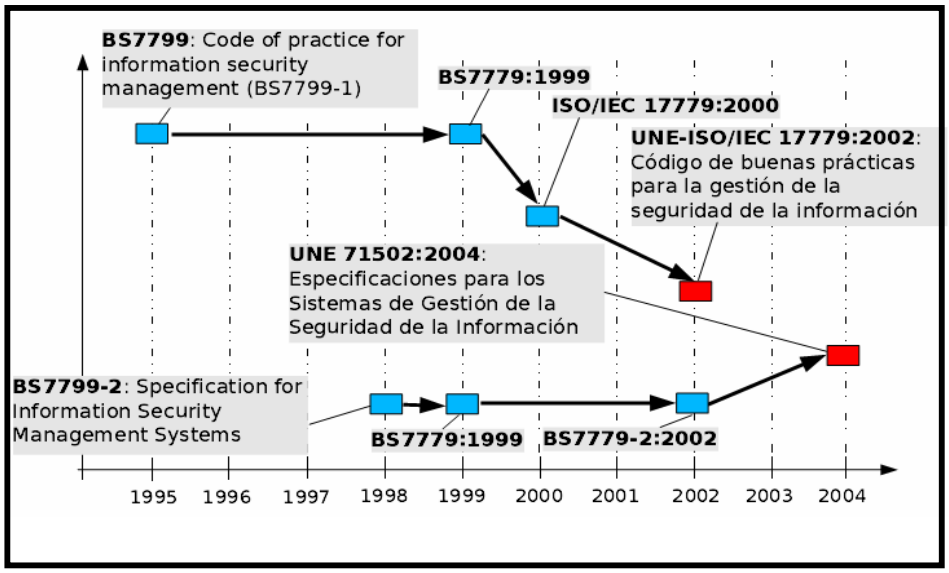

Figura 8.
Fuente: Villalón, (2005). Evolución del estándar ISO 17799.

Los controles de la ISO-17799

Para el éxito de la implementación del estándar de seguridad ISO-17799 se requiere de una serie de procedimientos donde, inicialmente, el análisis de riesgos identificará los activos de la información y las amenazas a las cuales se encuentra expuesta, para luego definir los controles que aplican a la organización con objeto de proporcionar niveles prácticos de seguridad de la información y medir el cumplimiento de los mismos.

El estándar ISO-17799, consta de diez dominios de seguridad:

Políticas de seguridad: El estándar define como obligatorias las políticas de seguridad documentadas, además de los procedimientos internos de la organización que permitan su actualización y revisión por parte de un Comité de Seguridad.

Organización de Seguridad: Establece el marco formal de seguridad que debe integrar una organización, tales como un foro de administración de la seguridad de la información, un contacto oficial de seguridad (Information

System Security Officer – ISSO), revisiones externas a la infraestructura de seguridad y controles a los servicios de outsourcing, entre otros aspectos.

Clasificación y control de activos: se deben identificar todos los activos de información importantes dentro de la organización. Asignar un responsable o propietario de esos activos. Clasificar la información de acuerdo con necesidad, prioridad y nivel de protección. Realizar un análisis de riesgos (ataques externos, intrusos, software ilegal, difusión de información, fraude informático, destrucción de hardware, etc.).

Seguridad del personal: proporcionar controles a las acciones del personal que opera con los activos de información.

El objetivo, reducir el riesgo inherente a la interacción humana, como robo, fraude o uso indebido de los recursos asignados. Establecer las responsabilidades mediante contratos, evaluación de antecedentes del personal, acuerdos de confidencialidad.

Seguridad física y ambiental: establecer los perímetros de seguridad, impedir acceso no autorizado a las instalaciones, salas, oficinas. Equipar y proteger instalaciones de cableado de telecomunicaciones, suministro eléctrico, que puedan propiciar la paralización de las funciones de la empresa.

Gestión de Comunicaciones y operaciones: establecer los procedimientos y responsabilidades operativas, planificar y aprobar sistemas, control de código malicioso, administraciones de red y seguridad de los medios de almacenamiento, control de cambios en la configuración de los equipos, manejo de incidentes.

Sistema de Control de accesos: definir los requerimientos del negocio, activar los mecanismos que permitan monitorear el acceso a los activos de información y el control de usuarios, establecer los procedimientos de definición de responsabilidades o perfiles de seguridad y el control de acceso a las aplicaciones, establecimiento de políticas para el acceso móvil o remoto.

Desarrollo y mantenimiento de sistemas: La organización debe disponer de procedimientos que garanticen la calidad y seguridad de los sistemas desarrollados para tareas específicas de la organización, definir procesos de criptografía, seguridad de los archivos, soporte y mantenimiento de sistemas.

Plan de Continuidad del Negocio: la administración de la seguridad debe indicar los procedimientos de recuperación en caso de interrupciones de las actividades del negocio, así como, asegurar los procesos críticos del mismo de fallas importantes o desastres. Probar, mantener y reevaluar de los planes de continuidad de los negocios.

Cumplimiento: La organización establecerá los requerimientos de seguridad para cumplir con los requisitos de las leyes, establecerá las normas que deben cumplir todos sus proveedores, socios y usuarios; éstos se encontrarán formalizados en los contratos o convenios. Equilibrio entre las políticas de seguridad y la compatibilidad técnica.

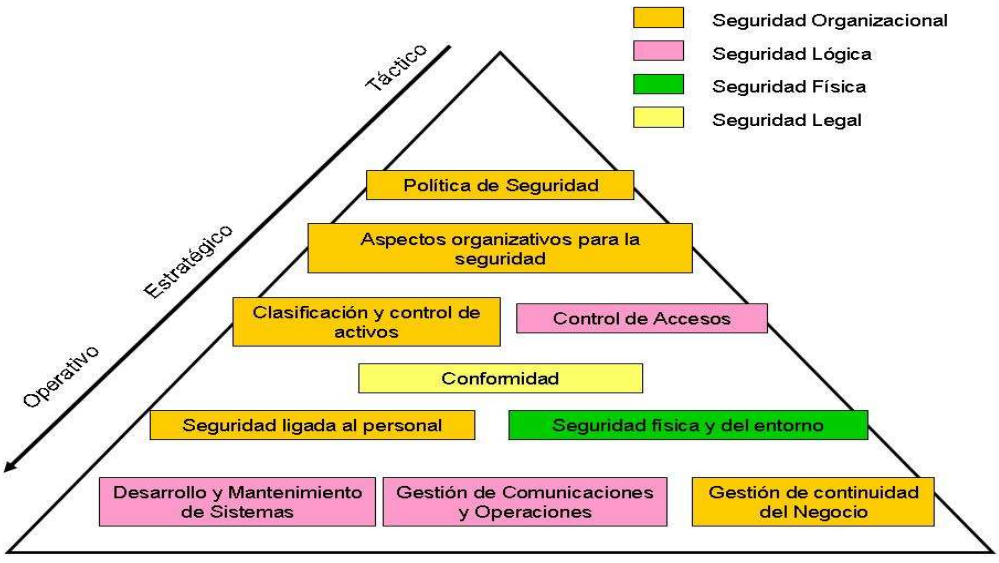

Figura 9.
Fuente: Tomado y adaptado, Villalón (2004). Dominios de la ISO-17799.

Cada uno de los dominios (ver figura 9), establece una serie de controles que serán seleccionados dependiendo de los resultados obtenidos en el análisis de riesgos, además, existen controles obligatorios para toda organización, como los de políticas de seguridad cuyo número dependerá más de la organización que del estándar, el cual no establece este nivel de detalle.

Beneficios que puede aportar la implementación de esta norma a una organización:

- Establecimiento de metodologías de gestión de la seguridad claras y estructuradas.
- Reducción del riesgo de pérdida, robo o corrupción de información.
- Los clientes tienen acceso a la información a través medidas de seguridad.
- Los riesgos y sus controles respectivos son continuamente revisados.
- Confianza de clientes y socios estratégicos por la garantía de calidad y confidencialidad comercial.
- Las auditorias externas ayudan a identificar las debilidades del sistema y las áreas que se pueden mejorar.
- El sistema se integra con otros sistemas de gestión (ISO9001, ISO14001, etc.).
- Continuidad de las operaciones necesarias de negocio tras incidentes de gravedad.
- Conformidad con la legislación vigente sobre información personal, propiedad intelectual y otras.
- Imagen de empresa a nivel internacional y elemento diferenciador de la competencia.
- Proporciona confianza y reglas claras a las personas de la organización.
- Reduce costes y mejora los procesos y el servicio.
- Aumenta la motivación y satisfacción del personal.
- Seguridad garantizada en base a la gestión de procesos en vez de en la compra sistemática de productos y tecnologías.

El estándar ISO 17799, es revisado en el 2005 y se producen algunos cambios, lo cuales serán recopilados en una nueva norma denominada ISO 27002. Además la ISO, trabaja en otros estándares diseñados para el área

de la seguridad de la información, los cuales se agruparan en la familia de las norma ISO 27000, de estos ya se publicó, el ISO 27001.

Olivares (2005), relaciona los cambios importantes dentro del estándar:

- Definiciones y términos
- Controles esenciales
- Factores críticos de éxito
- Estructura del estándar
- Contenido de los controles.
  - Dos nuevas cláusulas generales
  - Nueva cláusula de control (área de control o dominio de control)
  - Cláusulas, objetivos de control y controles modificados.

  Además incluye los aspectos nuevos dentro de la norma ISO 17799:
- Seguridad en los servicios externos y de outsourcing.
- Gestión de vulnerabilidades tecnológicas.
- Enfoque en la gestión de incidentes.
- Comunicaciones móviles, remotas y distribuidas en el tratamiento de la información.
- Clarificación en la evaluación y tratamiento del riesgo.
- Nuevos controles para la gestión de personal.
- Nuevos controles en relación con clientes y entrega de servicios.

Culminando con la descripción de las tareas de gestión y análisis de Riesgos en seguridad informática, es necesario mencionar que en la actualidad, todas estas funciones se están agrupando bajo lo que se conoce como SGSI (Sistemas de Gestión de la Seguridad de la información). Dado que la seguridad de la información, es un elemento que evoluciona rápida y continuamente, y se hace necesario el control y seguimiento de los procedimientos aplicados, en forma permanente.

BASES LEGALES

Los avances tecnológicos modernos, han requerido de controles legales para su uso y conformidad de acuerdo al país donde se apliquen. La seguridad informática moderna, necesita del apoyo de bases jurídicas que permitan, establecer responsabilidades y mecanismos de regulación para la aplicación de la misma. En Venezuela, el gobierno ha ido formulando Leyes y normativas referentes a las Tecnologías de la Información, con el objetivo de darle solidez y piso jurídico, a las antes mencionadas. A continuación se presentan las leyes que influyen o regulan, el aspecto relativo a la seguridad informática:

Plan Nacional de Tecnologías de la Información, (2001):

Menciona en el apartado de la situación actual de las TIC's en Venezuela, lo siguiente:

> "La situación cambia de manera significativa en el sector productivo. Uno de los sectores que han incorporado rápidamente sus servicios en línea y en estos momentos aprovechan al máximo las ventajas de Internet, son los medios de comunicación social, especialmente los medios impresos. Es posible decir lo mismo con respecto a la industria en el sector de las telecomunicaciones. En cambio, no es así en otros sectores productivos, como la industria manufacturera venezolana y la agroindustria. Desde el punto de vista del tamaño de las empresas, no cabe duda que la incorporación de las TIC en las grandes empresas es mucho mayor que en las PYME".
>
> Entre los lineamientos estratégicos de este plan se reseña en el **Ordinal D.** "Promover el uso de las tecnologías de información en el sector productivo, público y privado, a fin de elevar su productividad y competitividad, en el marco de la nueva economía"**.**
>
> (a) Promover los mercados, productos y servicios, en la economía mediante un adecuado marco jurídico y regulatorio.

(b) Establecer mecanismos de fomento que permitan la difusión de las Tecnologías de Información en las PYME y la generación de nuevos emprendedores, (...).

Este Plan describe la iniciativa del gobierno venezolano, por apoyar y desarrollar el mercado de TIC's para la Pequeña y Mediana Empresa, grupo de gran importancia para sector económico del país. A través del establecimiento de lineamientos objetivos que permitan el crecimiento de este conjunto empresarial.

Ley especial contra delitos informáticos:

Título I. Disposiciones Generales. Artículo 1.
Objeto de la ley. La presente ley tiene por objeto la protección integral de los sistemas que utilicen tecnologías de información, así como la prevención y sanción de los delitos cometidos contra tales sistemas o cualquiera de sus componentes o los cometidos mediante el uso de dichas tecnologías, en los términos previstos en esta ley.

Este instrumento legal viene a fortalecer el auge de las comunicaciones y el desarrollo de las tecnologías de la información en Venezuela. En él se regula todo lo referente a sistemas informáticos y a los posibles delitos que se cometan haciendo uso de los mismos.

Ley sobre mensajes de datos y firmas electrónicas:

CAPITULO I. Objeto y aplicabilidad del Decreto-Ley. Art. 1
El presente Decreto-Ley tiene por objeto otorgar y reconocer eficacia y valor jurídico a la Firma Electrónica, al Mensaje de Datos y a toda información inteligible en formato electrónico, independientemente de su soporte material, atribuible a personas naturales o jurídicas, públicas o privadas, así como regular todo lo relativo a los Proveedores de Servicios de Certificación y los Certificados Electrónicos.

El presente Decreto-Ley será aplicable a los Mensajes de Datos y Firmas Electrónicas independientemente de sus características tecnológicas o de los desarrollos tecnológicos que se produzcan en un futuro. A tal efecto, sus normas serán desarrolladas e

interpretadas progresivamente, orientadas a reconocer la validez y eficacia probatoria de los Mensajes de datos y Firmas Electrónicas.

Ley que apoya las transacciones a través de los formatos digitales, lo que permitirá desarrollar sobre bases legales, el comercio electrónico, la transferencia de datos entre organizaciones, el establecimiento de redes ínter empresariales, así como la comunicación efectiva entre organismos públicos y privados.

Ley Orgánica de Telecomunicaciones:

Titulo I, Disposiciones Generales:
Artículo 4.- Se entiende por telecomunicaciones toda transmisión, emisión o recepción de signos, señales, escritos, imágenes, sonidos o informaciones de cualquier naturaleza, por hilo, radioelectricidad, medios ópticos, u otros medios electromagnéticos afines, inventados o por inventarse. Los reglamentos que desarrollen esta Ley podrán reconocer de manera específica otros medios o modalidades que pudieran surgir en el ámbito de las telecomunicaciones y que se encuadren en los parámetros de esta Ley.

Titulo II, De los Derechos y Deberes de los Usuarios y Operadores.

Capitulo II, De los Derechos y Deberes de los Usuarios.
2. La privacidad e inviolabilidad de sus telecomunicaciones, salvo en aquellos casos expresamente autorizados por la Constitución o que, por su naturaleza tengan carácter público.

Ley que da soporte jurídico al área de las telecomunicaciones de la nación, servirá para regular la apertura de las telecomunicaciones en el país, reglamentando la transferencia de información entre los diferentes organismos, incluyendo las redes de datos (Redes de computadoras).

TÍTULO II, DISPOSICIONES GENERALES

Capitulo IV, De la seguridad de los sistemas y las redes, y del riesgo tecnológico Rectoría en materia de seguridad y riesgo tecnológico.

Artículo 36. El órgano rector de la materia de tecnologías de información conjuntamente con la Comisión Nacional de Tecnologías de Información desarrollará las políticas, lineamientos, normas y estándares técnicos que serán aplicables en la seguridad de las redes y de los sistemas de información así como los elementos de análisis y administración del riesgo tecnológico que deben observarse para la creación, mantenimiento y funcionamiento de los sistemas de información y de las redes.

Criterios de Seguridad

Artículo 37. A los fines del artículo anterior, se tendrán en cuenta los siguientes criterios de seguridad tecnológica:

1. Prever los mecanismos y herramientas de evaluación, detección, acción y control, que permitan evaluar, detectar y corregir vulnerabilidades de las plataformas y sistemas.
2. Administrar las capacidades para garantizar los requerimientos tecnológicos que demanden los servicios que se ofrecen.
3. Manejar la seguridad lógica y física sobre los componentes, contenidos, aplicaciones, sistemas, servicios, redes, plataforma, infraestructura tecnológica y la instalación física de alojamiento.
4. Proporcionar niveles de confidencialidad que garanticen la inviolabilidad del carácter privado de la información a través del uso de certificados y firmas electrónicas.
5. Prever políticas y mecanismos de auditoria constante y periódica a los fines de realizar evaluación y seguimiento a las soluciones tecnológicas.
6. Establecer planes de contingencia y de recuperación de operaciones, así mismo, contemplar lo relativo a los respaldos y recuperación de almacenamiento de la data.
7. Garantizar que los componentes, servicios y aplicaciones puestos a disposición de los ciudadanos cuenten con elementos de calidad en todos los niveles.
8. Garantizar la prestación de servicios al ciudadano y el disfrute del acceso al servicio en las mejores y más óptimas condiciones: oportunidad, disponibilidad y rendimiento, entre otras.

TITULO VI
DERECHOS Y GARANTÍAS DE LOS CIUDADANOS
Carácter confidencial y privado de la información.
Artículo 66. La información sobre la vida privada e intimidad de las personas es de carácter confidencial y privado. Los datos personales asentados en archivos, registros, bases de datos, u otros medios electrónicos de tratamiento de datos, estarán íntegramente protegidos para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en los artículos 28, 60 y 143 de la Constitución Nacional.

Ley para el establecimiento, control, y desarrollo de las tecnologías de la información en el país, además de incluir un apartado hacia el aseguramiento de la información por parte de sus propietarios. Esta ley establece lineamientos claros a seguir para la protección de la información por parte de todas las organizaciones que utilizan TIC's para el apoyo de sus operaciones, donde se establece el carácter privado y confidencial de la información, salvo las excepciones indicadas por las leyes de la república.

DEFINICIÓN DE TERMINOS

En este apartado se definen los términos que se relacionan con el área de la seguridad y riesgos informáticos, con el objeto de aclarar la utilización de los mismos dentro del ámbito antes mencionado.

- **Certificado digital:** Laudon (2002), lo refiere como un anexo a un mensaje electrónico que verifica la identidad del remitente y proporciona al destinatario un mecanismo para codificar su respuesta.
  Oz (2002), lo define como una tarjeta de identificación física que contiene una clave pública y una firma digital. Los certificados digitales son expedidos por empresas o autoridades certificadas, confiables al público.
- **Firma digital:** Oz (2002), lo describe como un código digital que solo identifica al remitente de un mensaje. Es un elemento importante en el comercio electrónico en Internet. Los negocios lo usan para identificar compañías e individuos que ejecutan transacciones financieras y de otro tipo.
- **Criptografía:** Ramió (2006), la define como: rama inicial de las Matemáticas y en la actualidad de la Informática y la Telemática, que hace uso de métodos y técnicas con el objetivo de cifrar, y por tanto proteger, un mensaje, archivo o datos, por medio de un algoritmo, usando una o más claves.
- **Cifrado de Datos:** Ramió (2006), es una técnica que, protege o autentica a un documento o usuario aplicando algoritmos criptográficos. Y que sin conocer una clave específica o secreta, no será posible descifrarlos o recuperarlos.
- **Firewall:** Borghello (2001), dispositivos que permiten bloquear o filtrar el acceso entre dos redes, puede ser entre una red privada y una red externa como Internet o una Extranet. Permiten la salida al exterior y a su vez previenen de intromisiones hacia el interior de la red. Pueden ser físicos o lógicos.

- **Ingeniería Social:** técnica utilizada para engañar a un usuario de una organización y de esta manera obtener su clave de acceso a los sistemas de la empresa, de una forma “amigable”.
- **Spam:** publicidad no deseada, que generalmente llega a los buzones de correo electrónico, si haberla solicitado.
- **Spyware:** es un software creado para espiar o extraer información de un computador victima y luego enviarla a otros, sin que el usuario o dueño se entere o lo autorice.
- **Phising:** estafa electrónica, la cual puede ocurrir mediante el uso de correos electrónicos engañosos, o páginas Web fraudulentas diseñadas para confundir a los usuarios, de forma tal que estos proporcionen su información personal y financiera como puede ser: nombres completos, Nro. De identificación, Nro. de Tarjeta de crédito, nombres de usuario, contraseñas de acceso a cuentas.

SISTEMA DE VARIABLES

Definición Conceptual de la Variable:

Para la investigación, se define la variable Riesgos de seguridad informática, la cual es definida por Izquierdo (2005), como, “una probabilidad de que una amenaza explote vulnerabilidades de un activo o conjunto de activos de la información y cause perdida o daño a los mismos”.

Definición Operacional de la Variable:

La definición operacional de la variable se realiza, tomando en cuenta el objetivo principal de la investigación, relacionándolo a su vez, con los objetivos específicos, para luego dimensionar cada uno de ellos de acuerdo con los, riesgos, herramientas de control y lineamientos a seguir para instaurar seguridad de la información. Logrando, de esta manera determinar los indicadores, que permitan construir los instrumentos de medición y recolección de datos de la investigación.

A continuación se presenta un cuadro (ver cuadro 5), donde se puede apreciar la operacionalización de las variables para el problema en estudio.

Cuadro 5: Operacionalización de las Variables de la investigación.

Objetivo General	Objetivos Específicos.	Dimensiones	Indicadores	Ítems
Analizar los Riesgos de Seguridad Informática en las Pequeñas y Medianas Empresas (PyME's), usando el Estándar ISO-17799 para la definición de políticas de seguridad que protejan sus Sistemas de Información	(1) Identificar las situaciones de riesgo que afectan la seguridad informática, tomando como referencia la norma ISO-17799, en los sistemas de información que sirven de apoyo a las PyME's.	◆ Riesgos	⅄ Sistemas y software en uso en la empresa. ⅄ Permisos para acceso a la información. ⅄ Normas para el uso de la información y equipos de computación.	12,13, 14 2,17,18 1,2,6,16
		◆ Amenazas	⅄ Normas para respaldo de datos. ⅄ Control de acceso a sistemas de información	2, 11 15,16,17,18
		◆ Vulnerabilidades	⅄ Control de acceso y seguridad física de las instalaciones de la empresa. ⅄ Pólizas de seguros.	7,8,9 22

Fuente: Elaboración propia, Villasmil (2006).

Cuadro 5 (continuación)**.** Operacionalización de las Variables de la investigación

Objetivo General	Objetivos Específicos.	Dimensiones	Indicadores	Ítems
Analizar los Riesgos de Seguridad Informática en las Pequeñas y Medianas Empresas (PyME's), usando el Estándar ISO-17799 para la definición de políticas de seguridad que protejan sus Sistemas de Información.	(2) Determinar las herramientas necesarias para el control de la seguridad informática, a través del análisis, categorización y monitoreo de los riesgos que afectan a los sistemas de información que apoyan a las PyME's	◆ Controles para aplicaciones	⅄ Uso de antivirus. ⅄ Uso de Firewalls	12 13
		◆ Auditorias de Sistemas y Control interno	⅄ Auditoria de sistemas e identificación de problemas. ⅄ Políticas de seguridad para uso de la información. ⅄ Conocimiento de las normas jurídicas para el uso de la información.	19,20 1,2,3,10, 21 24
	(3) Proponer un conjunto de lineamientos sobre seguridad informática, basados en el estándar ISO-17799, que se adapten a las necesidades de las PyME's y que contribuyan a mejorar funcionamiento de sus sistemas de información.	◆ Lineamientos de la norma ISO-17799.	⅄ Conocimiento de la norma ISO-17799. ⅄ Políticas documentadas para el uso de la información. ⅄ Asignación de responsabilidades en materia de seguridad de la información.	23 1,2,19,20 4,5

Fuente: Elaboración propia, Villasmil (2006).

CAPITULO III
MARCO METODOLÓGICO

Toda investigación científica, requiere de una metodología previa que le indique al investigador, los pasos necesarios para lograr los objetivos propuestos en la investigación. Este capitulo refiere todo lo relacionado con los principios metodológicos que se usaron en el estudio planteado.

Diseño y Tipo de la Investigación

El diseño de la investigación es, no experimental, apoyada en un estudio de campo, de nivel descriptivo, según lo definido por Sabino (1992):

> En los diseños de campo los datos de interés se recogen en forma directa de la realidad, mediante el trabajo concreto del investigador y su equipo. Estos datos, obtenidos directamente de la experiencia empírica, son llamados primarios, denominación que alude al hecho de que son datos de primera mano, originales, producto de la investigación en curso sin intermediación de ninguna naturaleza.

En tal sentido, la investigación propuesta ha sido identificada como "Análisis de los Riesgos de Seguridad Informática, para las Pequeñas y Medianas Empresas (PyME's) usando el estándar ISO-17799, para la definición de políticas de seguridad que protejan sus Sistemas de Información". Situación importante hoy día, donde las nuevas tecnologías de la información y comunicaciones, se han integrado activamente en las organizaciones.

Continuando con los detalles sobre la metodología, la misma es descriptiva, la cual según Hernández y otros (2004), tiene como objetivo: "especificar las propiedades características y rasgos importantes de cualquier fenómeno que se analice".

Tales planteamientos, permiten al investigador, evaluar y proponer lineamientos que contribuyan a reducir los riesgos informáticos y mejorar la seguridad informática existente en las pequeñas y medianas empresas.

Población y Muestra

Población:

La población es definida por Hernández y otros (2004), como:"Conjunto de todos los casos que concuerdan con determinadas especificaciones".

En tal caso, para la presente investigación, se define la población objeto a partir de lo anteriormente expuesto. Por lo que se considera, que para el estudio propuesto la población estará representada por todas las empresas tipo PyME's, que se encuentren ubicadas en la zona industrial de Barquisimeto. Según la Cámara de Pequeños y medianos industriales del Estado Lara (CAPMIL), para el primer semestre del año 2006, es de 145 empresas activas y solventes.

Muestra:

Motivado a que la población objeto del estudio es finita, se necesita para la investigación la selección de una muestra. Basándose en la definición de muestra que proporciona Sabino (1992): la cual dice "Es una parte del todo que llamamos universo (población) y que sirve para representarlo". A los efectos de esta investigación, para determinar la muestra se usa, el muestreo aleatorio simple con un nivel de 95% de confianza. Por consiguiente, el tamaño de la muestra queda definido en un total de 30 empresas tipo PyME's.

Técnicas de Recolección de Datos

Una vez definido el diseño de la investigación, es necesario especificar las técnicas o instrumentos que permitan recolectar los datos necesarios para cumplir con los objetivos de la investigación. En referencia a lo anterior Sabino (1992), define Instrumento de recolección de datos como: "cualquier recurso del que se vale el investigador para acercarse a los fenómenos y extraer de ellos información". De forma que para el presente estudio se procedió de la siguiente manera:

- Elaboración de un cuestionario apoyado en el cuadro de operacionalización de las variables, a fin de ser entregado a los integrantes de la muestra.

Por otra parte, Hernández y otros (2004), definen cuestionario como un "Conjunto de preguntas respecto a una o más variables a medir". En este sentido, para la recolección de la información requerida, se aplica un cuestionario, de preguntas (Cerradas) con varias alternativas a seleccionar.

Validez del Instrumento

Para poder aplicar el instrumento de recolección de datos, este primeramente es validado, lo cual se realizó mediante juicio de expertos, lo que consiste según Balestrini (1997) en:

> Una vez definido y diseñado los instrumentos y procedimientos de recolección de los datos, atendiendo al tipo de estudio, antes de aplicarlos de forma definitiva en la muestra seleccionada, es conveniente someterlos a prueba, con el objetivo de establecer su validez en relación con el problema investigado.

Para realización de la validación del instrumento de recolección de

datos, se tomó en cuenta la opinión de tres profesionales, dos expertos con experiencia en Tecnologías de la Información y comunicaciones y un métodologo.

Técnicas de Análisis de Datos

En esta fase se procede a la clasificación, análisis e interpretación de la información recolectada. Balestrini (1997), comenta: “es una etapa de carácter técnico, pero de reflexión, que involucra la introducción de técnicas adecuadas la para la organización de la información”.

En atención al análisis e interpretación de los resultados, se utiliza como método la estadística descriptiva, la cual permite a través de cálculos estadísticos de frecuencias absolutas y porcentuadas, para obtener los resultados sobre la información recolectada que se correspondan con los ítems o variables planteadas en el instrumento de recolección de datos, aplicado a la muestra seleccionada.

Presentación de los Resultados

La presentación de los resultados del estudio se hace a través de gráficos estadísticos de columnas y análisis, que permiten aclarar los alcances obtenidos en la investigación.

CAPITULO IV
ANALISIS E INTERPRETACIÓN
DE LOS RESULTADOS OBTENIDOS

Una vez concluida la fase de recolección de los datos, en una investigación científica, es necesario que se analice, interprete y se presente la información obtenida. Este Capitulo trata lo relacionado con el análisis e interpretación de los resultados encontrados en el estudio propuesto.

Luego de aplicarse el instrumento de recolección datos, que se diseño para la investigación en estudio, que trata sobre los Riesgos de Seguridad Informática, él cual se desarrolló en las Pequeñas y Medianas Empresas (PyME's), se presenta a continuación la información recaudada.

La presentación de la información se hace a través de gráficos, donde se consideraron los ítems con mayor frecuencia de respuesta, dentro de la encuesta aplicada a las empresas seleccionadas.

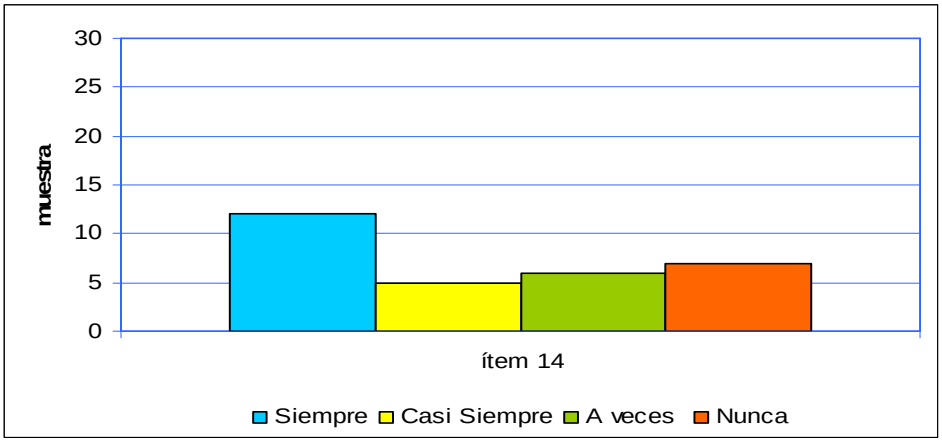

Grafico Nro. 1. Riesgos que afectan la seguridad informática. Indicador: Sistemas y software en uso.
Fuente: Elaboración propia, Villasmil (2006).

El gráfico Nro. 1, señala los resultados, del indicador sistemas y software en uso en la empresa, el ítem 14 muestra que un 40% de las empresas encuestadas siempre utilizan herramientas para chequear y monitorear sistemas y redes de computadoras, 17% casi siempre lo hace, un grupo de empresas que representa el 20%, las usa a veces, mientras que un 23% nunca utiliza este tipo de herramientas. De acuerdo con el resultado obtenido, se puede inferir que en las PyME's no es muy común este tipo de utilidades, las cuales colaboran para el control y disminución de riesgos informáticos.

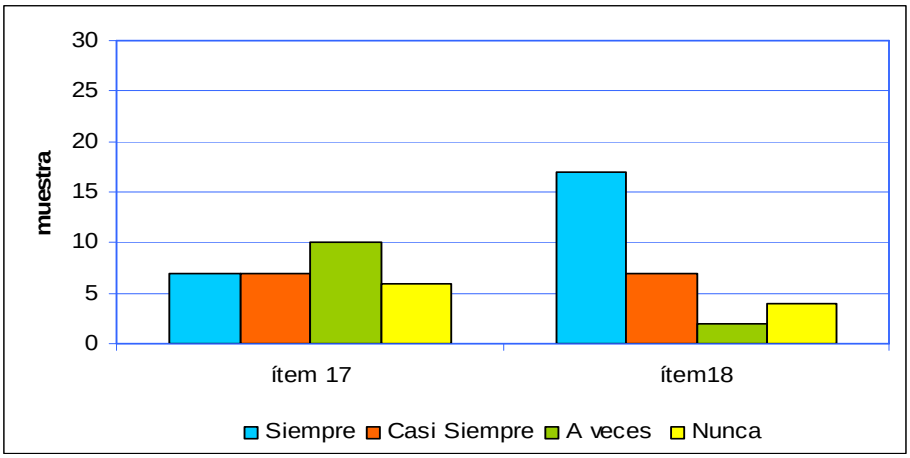

Grafico Nro. 2. Riesgos que afectan la seguridad informática. Indicador: Permisos para acceso a la información.
Fuente: Elaboración propia, Villasmil (2006).

El gráfico Nro. 2, expresa los resultados que se relacionan con el indicador Permisos para acceso a la información, el ítem 17, corresponde al acceso a Internet por parte de los usuarios de las PyME's donde la mayor parte de las empresas encuestadas que corresponde a un 33%, permite a veces este tipo de acceso a todos sus usuarios, un 20% respondió que nunca el acceso a este servicio es libre para todos los usuarios de las empresas, mientras que para las alternativas siempre y casi siempre fueron seleccionadas por un 23% de los consultados respectivamente . En cuanto al ítem 18, que trata sobre la inclusión o requerimientos de seguridad dentro de

los sistemas de información, la mayoría representada por un 57%, respondió que sus sistemas de información siempre tienen estos controles establecidos, 23% manifestó que casi siempre los sistemas tienen incluidos los requerimientos para la seguridad de la información, un 7% respondió que a veces están incluidos, mientras que un grupo del 13% no los aplica con regularidad. Lo que permite deducir que no todas las empresas controlan adecuadamente el acceso a su información.

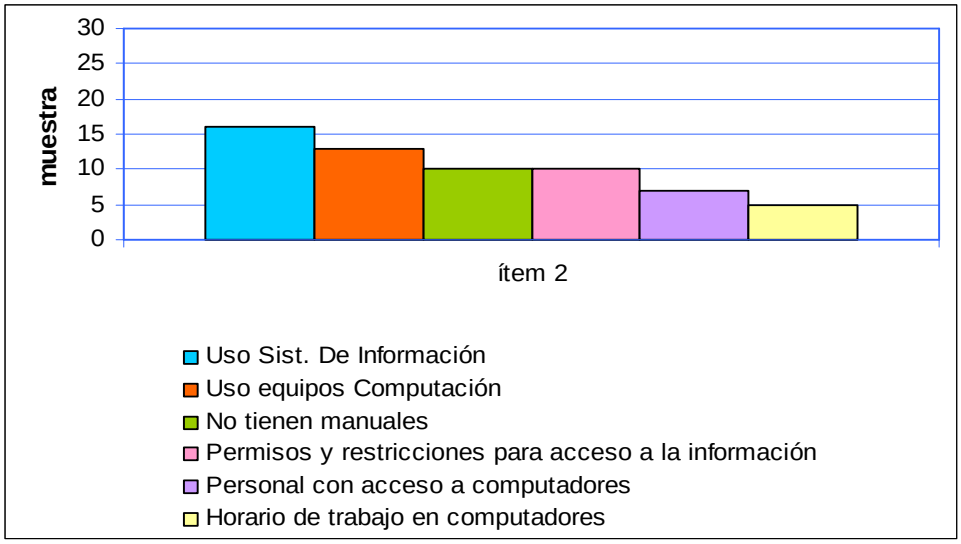

Grafico Nro. 3. Riesgos que afectan la seguridad informática. Indicador: Permisos para acceso a la información.
Fuente: Elaboración propia, Villasmil (2006).

El gráfico Nro. 3, presenta los datos que se relacionan con el ítem 2, correspondiente al uso de los manuales de normas y procedimientos, dedicados al área de sistemas, en el cual se puede apreciar, que un 53% de las empresas le dan prioridad a los Manuales de Sistemas de Información, además se puede notar, que hay un número significativo de empresas que corresponde a un 33%, las cuales no tienen manuales para esta área, un 43% de la muestra contesto que sí utilizan manuales para el uso de los equipos de computación, 33% seleccionaron poseer los manuales para establecer los permisos y restricciones de acceso a la información, 23%

contesto que poseen manuales para indicar el personal con acceso a los computadores, mientras que el 17% selecciono la opción horario de trabajo en los equipos de computación; de lo anterior se desprende que el uso de manuales y normas para el área de informática, no es algo de uso común dentro de las empresas estudiadas, pudiéndose considerar un riesgo en cuanto a la seguridad informática.

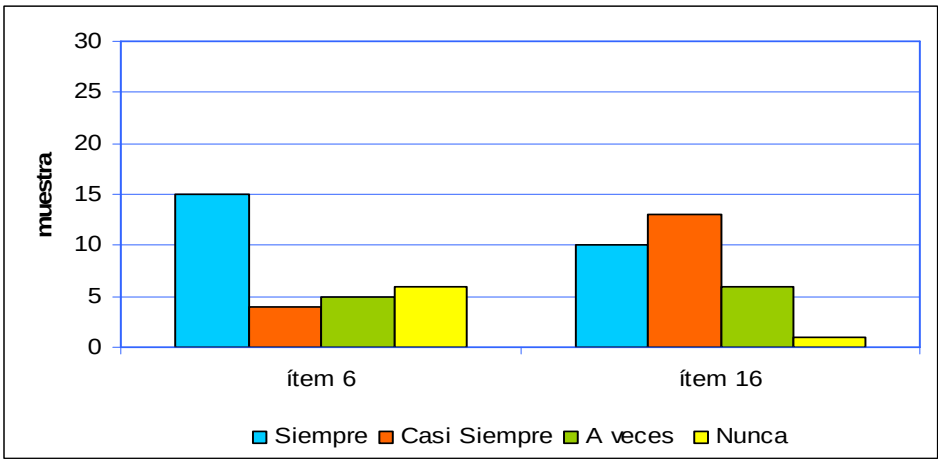

Grafico Nro. 4. Riesgos que afectan la seguridad informática. Indicador: Normas para el uso de la información y equipos de computación.
Fuente: Elaboración propia, Villasmil (2006).

En el gráfico Nro 4, se puede observar el comportamiento del ítem 6, que corresponde al establecimiento de acuerdos de confidencialidad, encontrándose que un 50% del grupo estudiado, admitió que siempre manejan este tipo de acuerdos, 13% indico que casi siempre usan este tipo de convenios, un 17% manifestó que a veces hacen uso de ellos, mientras que un 20% respondió que nunca hacen uso de esta modalidad para asegurar la información. El ítem 16 se refiere a la frecuencia de cambio para claves de acceso, donde un 43% casi siempre cambia con regularidad las claves de acceso a los sistemas, mientras que 20% lo hace a veces, un 33% de los encuestados siempre hace cambio de claves y un 3% nunca hacen cambio de claves de acceso para ingreso a los sistemas, pudiéndose

deducir que este grupo empresarial se preocupa por aplicar estas medidas de seguridad para su información.

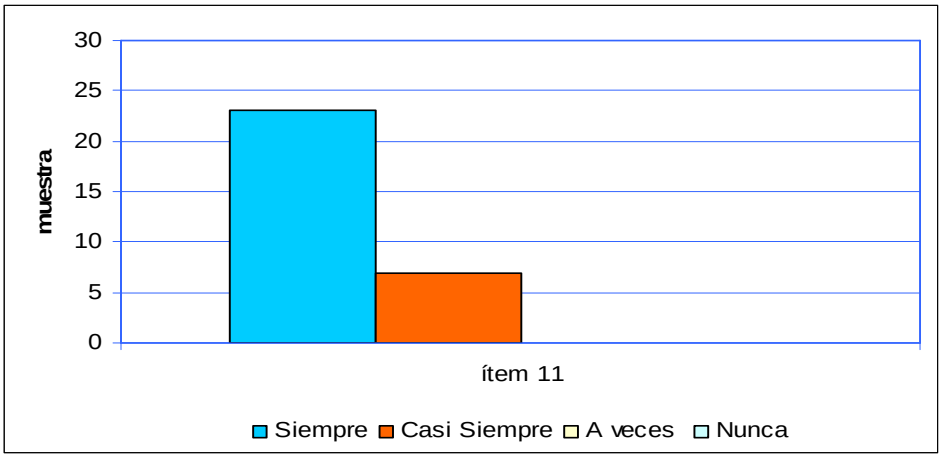

Grafico Nro. 5. Amenazas que afectan la seguridad informática. Indicador: Normas para el respaldo de datos.
Fuente: Elaboración propia, Villasmil (2006).

El gráfico Nro. 5, muestra los resultados obtenidos para el ítem 11, que se relaciona con la frecuencia de respaldo de archivos o base de datos, donde se puede apreciar que un 77% de la muestra estudiada siempre realiza esta tarea, mientras que un 23% respondió que casi siempre hacen los procesos de respaldo de información, induciendo que esta es una norma común en las empresas estudiadas.

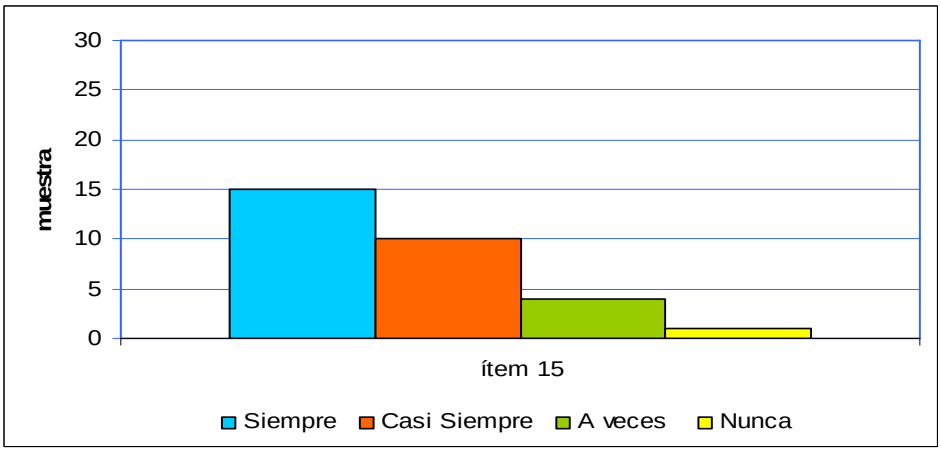

Grafico Nro. 6. Amenazas que afectan la seguridad informática. Indicador: Control de acceso a sistemas de información.
Fuente: Elaboración propia, Villasmil (2006).

En el gráfico Nro. 6, se muestran los resultados para el ítem 15, donde se indica que un 50% de las empresas en estudio, siempre verifica la confiabilidad y acceso a sistemas de información, 33% lo hacen casi siempre, un 13% lo realiza a veces y un 3% nunca realizan este tipo de chequeo o verificación, lo que indica que las rutinas de control y verificación para los sistemas de información de las PyME's es un proceso de uso regular.

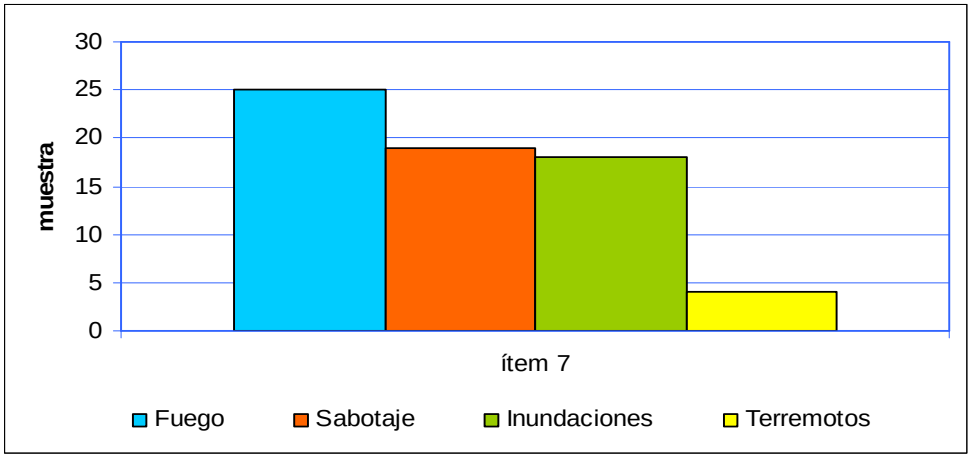

Grafico Nro. 7. Vulnerabilidades que afectan la seguridad informática. Indicador: Control de acceso y seguridad física de las instalaciones de la empresa.
Fuente: Elaboración propia, Villasmil (2006).

El gráfico Nro. 7, permite observar que entre los principales controles que usa la PyME, para la protección de las instalaciones físicas, se encuentra la protección contra fuego, la cual fue seleccionada por 83% de los encuestados, mientras que 63% aplica medidas de protección contra el sabotaje, otro de los controles usado es la prevención contra inundaciones, representado por 60% de grupo estudiado y un 13% manifestó proteger sus instalaciones contra sismos o terremotos. En consecuencia se puede deducir que las PyME's, no toman en cuenta todas las vulnerabilidades a las que están expuestas sus instalaciones físicas.

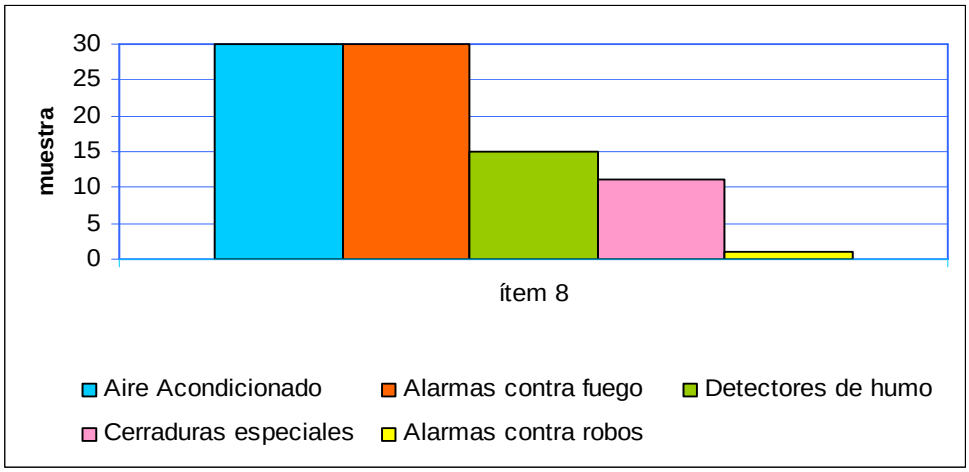

Grafico Nro. 8. Vulnerabilidades que afectan la seguridad informática. Indicador: Control de acceso y seguridad física de las instalaciones de la empresa.
Fuente: Elaboración propia, Villasmil (2006).

En el gráfico Nro. 8, se muestra cuales mecanismos de protección son los más usados por las PyME's, notándose que todas respondieron afirmativamente para el uso de aire acondicionado y alarmas para la detección de fuego, un grupo que representa 50% de los encuestados utiliza detectores de humo, las cerraduras especiales son usadas solo por 37% de la muestra estudiada y un pequeño grupo representado por 3% usa alarmas contra robos, por consiguiente se puede inferir que este grupo empresarial utiliza los mecanismos de protección tradicionales para sus instalaciones físicas.

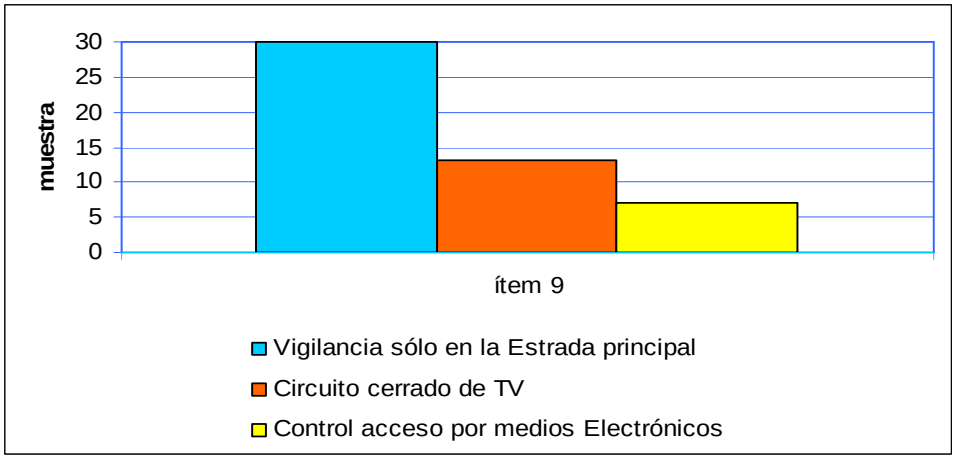

Grafico Nro. 9 Vulnerabilidades que afectan la seguridad informática. Indicador: Control de acceso y seguridad física de las instalaciones de la empresa.
Fuente: Elaboración propia, Villasmil (2006).

El gráfico Nro. 9 detalla el ítem 9 relacionado con el control de acceso a las instalaciones empresariales, pudiéndose notar que todos los integrantes de la muestra utilizan como medio de control la vigilancia en la entrada principal, un grupo de 43% tiene instalado circuito cerrado de TV como medida de seguridad y 23% de los encuestados manifestó usar el control de acceso a través de medios electrónicos, de lo cual se puede deducir que la PyME necesita modernizar sus medios para controlar el acceso a sus instalaciones físicas.

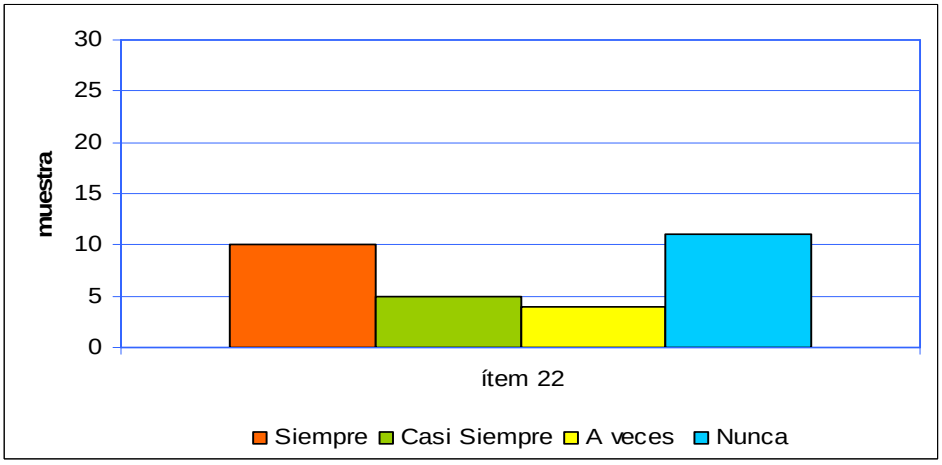

Grafico Nro. 10. Vulnerabilidades que afectan la seguridad informática. Indicador: Control de acceso y seguridad física de las instalaciones de la empresa.
Fuente: Elaboración propia, Villasmil (2006).

El gráfico No. 10, muestra ítem 22 relacionado con la adquisición de pólizas de seguro para los equipos de computación, donde el 37% respondió que nunca adquiere este tipo de seguro, un 33% menciono que siempre lo adquieren, un 17%, casi siempre se incorporan a un tipo de seguro para sus equipos de computación, mientras que un 13% lo hace a veces. Percibiéndose que la mayoría de la muestra en estudio no toma en cuenta este tipo de medidas para la seguridad física y ambiental de sus empresas.

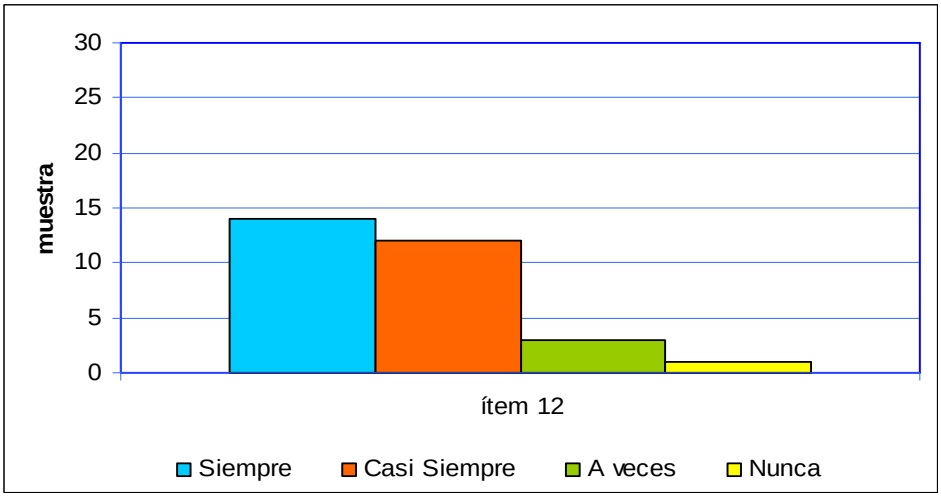

Grafico Nro. 11. Controles para aplicaciones. Indicador: Uso de antivirus.
Fuente: Elaboración propia, Villasmil (2006).

En el gráfico Nro. 11, se describe el ítem 12 relacionado con el uso, actualización de antivirus y software dentro de las PyME's estudiadas, encontrándose que un 47% de los consultados, siempre utiliza y actualiza sus antivirus, un 40% casi siempre lo hace, mientras que un 10% lo realiza a veces y un 3% nunca realiza estas tareas. Lo que hace presumir que las empresas tienen como prioridad la adquisición y actualización del software que poseen instalado dentro de su plataforma informática.

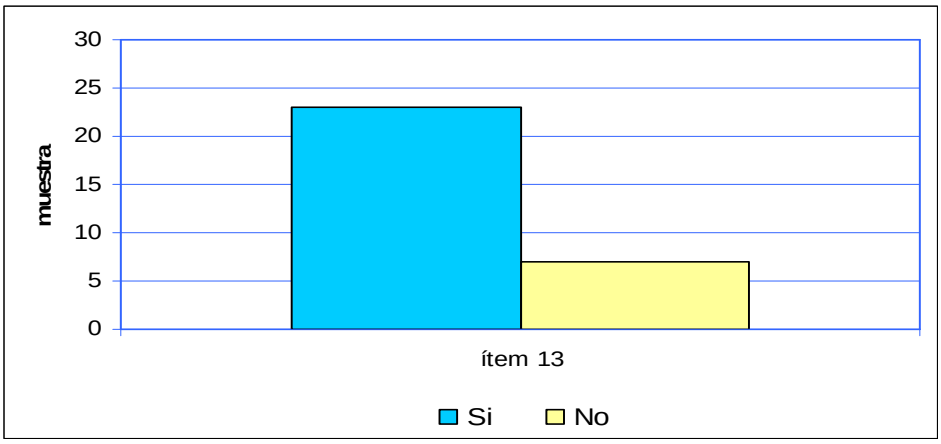

Grafico Nro. 12. Controles para aplicaciones. Indicador: Uso de Firewalls.
Fuente: Elaboración propia, Villasmil (2006).

El gráfico Nro. 12, muestra el ítem 13 relacionado con la utilización de Firewalls por parte de las PyME's, para controlar los accesos externos a sus redes de computadoras, pudiéndose notar que este es un dispositivo de uso frecuente, dado que la mayoría representada por un 77%, respondió afirmativamente, pero hay un grupo de las empresas que aun no lo utilizan representadas por un 23%.

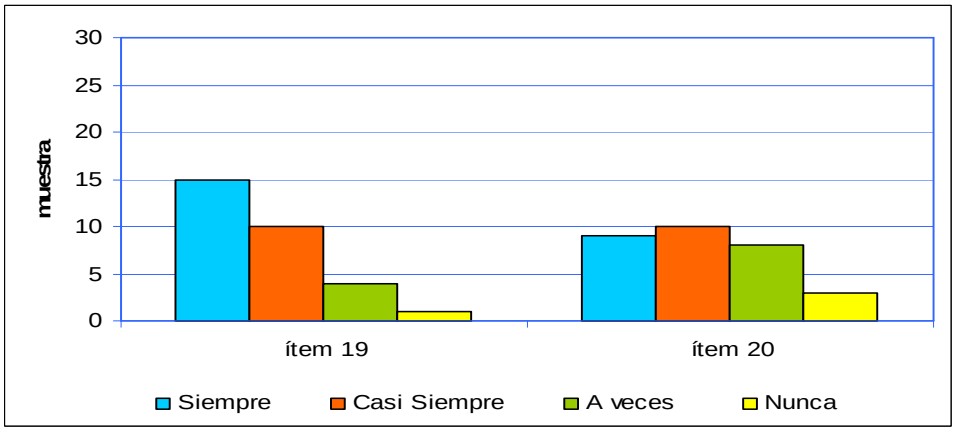

Grafico Nro. 13. Auditorias de Sistemas y Control Interno. Indicador: Auditoria e identificación de problemas.
Fuente: Elaboración propia, Villasmil (2006).

En el gráfico Nro. 13, se presenta el indicador auditoria e identificación de problemas dentro de los sistemas de información de una empresa PyME; el ítem 19 corresponde a la identificación de problemas o anormalidades en la plataforma informática, donde el 50% de los consultados manifestó siempre detectarlos, 33% respondió que casi siempre lo hace, un 13% selecciono la opción a veces y un 3% manifestó que nunca detecta este tipo de problemas. El ítem 20 se relaciona con la auditoria para los sistemas de información, donde 30% de la muestra indico que siempre se auditan los sistemas de información, 33% manifestó que casi siempre se hace, 27% respondió que a veces se realiza este proceso y un 10% nunca hacen auditorias para sus sistemas. De lo anterior se puede deducir que las PyME's, se ha comenzado a preocupar por el funcionamiento interno de sus sistemas de información y los auditan, con regularidad

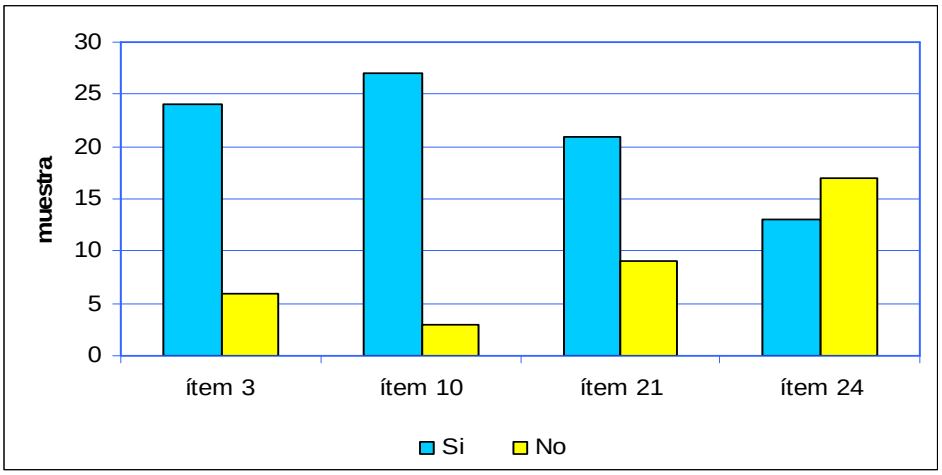

Grafico Nro. 14. Auditorias de Sistemas y Control Interno. Indicador: Políticas para la seguridad de la información y conocimiento sobre normativa jurídica para la información.
Fuente: Elaboración propia, Villasmil (2006).

El gráfico Nro. 14, muestra algunas de las políticas de seguridad para el uso de la información; el ítem 3 se relaciona con los inventarios de hardware y software donde el 80% afirmo realizarlos, mientras que un 20% no los hace. El ítem 10 se refiere a el uso de UPS o baterías para los computadores, donde un 90% menciono que si las utiliza y un 10% no hace

uso de este dispositivo de protección; el ítem 21 corresponde a la existencia de un plan alterno para el funcionamiento de la empresa en caso de problemas con la plataforma informática, donde se obtuvo un 70% de respuestas afirmativas y un 30% de respuestas negativas con relación a la pregunta; el ítem 24 se refiere al conocimiento de la normativa jurídica para la seguridad de la información que existe en el país, por parte de la PyME's, donde la muestra estudiada revelo que un porcentaje importante representado por 57%, no conoce dicha normativa y un 43% si esta al tanto de estos instrumentos legales. En consecuencia se puede decir, que la mayor parte de las empresas estudiadas, sí tienen políticas para la protección de su información.

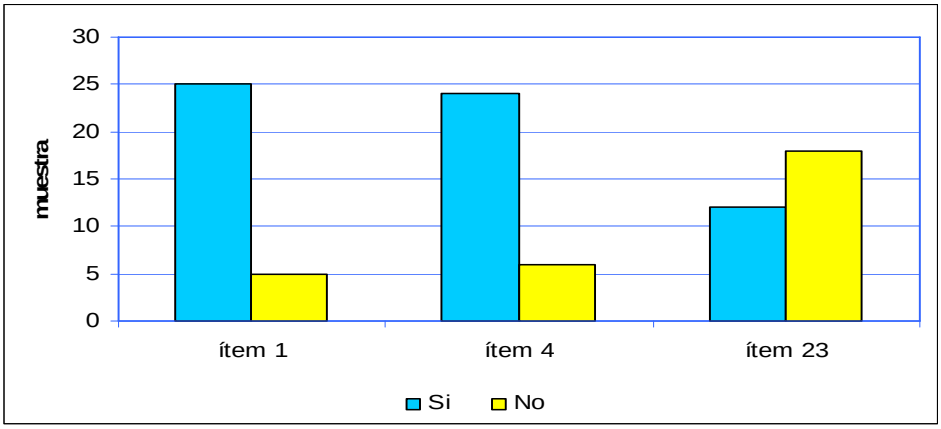

Grafico Nro. 15. Lineamientos de la Norma ISO-17799. Indicadores: Conocimiento de la norma, Políticas documentadas para la seguridad de la información y Asignación de responsabilidades en seguridad de la información.
Fuente: Elaboración propia, Villasmil (2006).

En el gráfico Nro. 15, se presenta la información que corresponde a los ítems de políticas de seguridad para la información (ítem 1), donde se encontró que un 83% de los encuestados respondió que sí las tienen establecidas, mientras que un 17% manifestó no tenerlas. El ítem 4 se relaciona con el personal que esta encargado del aseguramiento de la información, a este ítem respondió positivamente 63% de los consultados, mientras que el 37% no tiene personal asignado a esta área; el ítem 23

referido al conocimiento de las empresas en estudio sobre el estándar ISO-17799, en donde se encontró que un 60%, no tienen conocimiento sobre el mencionado estándar, aunque un 40% manifestó conocerlas. De lo anterior se puede deducir que la mayoría de los encuestados tienen políticas de seguridad de la información, pero desconocen las normas ISO-17799.

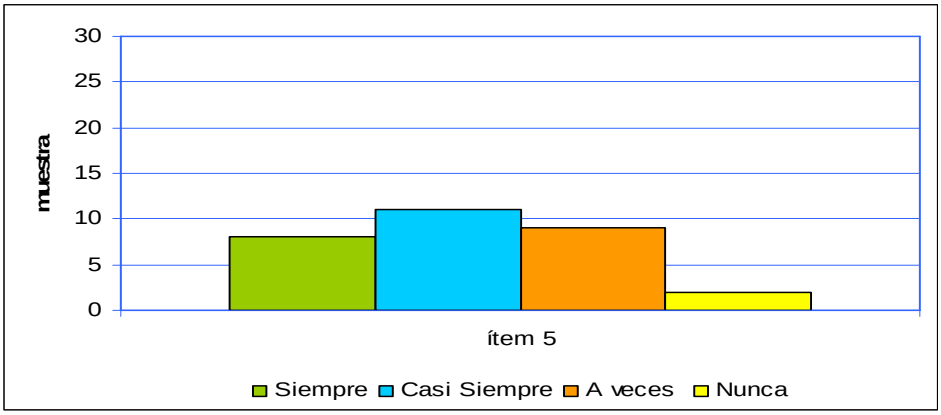

Grafico Nro. 16. Lineamientos de la Norma ISO-17799. Indicadores: Asignación de responsabilidades en seguridad de la información.
Fuente: Elaboración propia, Villasmil (2006).

En el gráfico Nro. 16, se muestra el ítem 5, relativo a la capacitación del personal de sistemas encargado de la seguridad de la información, donde se puede apreciar que un 37% de la muestra consultada, casi siempre capacita a su personal, un 30% lo hace a veces, un 27% lo realiza siempre, mientras que un 7% no lo realiza nunca, indicando que la mayoría de los integrantes del estudio se preocupan por contar con un personal capacitado y actualizado en materia de sistemas de información.

Los resultados de la investigación, muestran que el grupo empresarial de las PyME's, ha comenzado la adaptación a las nuevas tecnologías de la información, pero aun le falta fortalecer los procedimientos y normativas para el aseguramiento de la misma.

CAPITULO V
CONCLUSIONES Y RECOMENDACIONES

Las investigaciones científicas, proporcionan valiosa información que puede servir de base a otros estudios, para lo cual siempre es necesario elaborar los planteamientos que permitan hacer un cierre sobre el estudio, además de contribuir con recomendaciones o sugerencias de acuerdo con la problemática investigada.

Conclusiones

De acuerdo con las directrices de la investigación, y tomando como referencia el análisis e interpretación de los resultados, se presentan las siguientes conclusiones:

- Se ha encontrado que la mayoría de las empresas encuestadas, tienen instalados niveles de protección simple para sus sistemas de información, lo que conlleva a que enfrenten riesgos para su información.
- Un gran número de las empresas estudiadas, tienen establecidas políticas para la seguridad de la información, pero aun no son del conocimiento de toda la organización.
- Se pudo observar que entre las PyME's estudiadas se utilizan poco los manuales para el área de sistemas de información, lo que podría causar desconocimiento sobre la normativa que existe para el trabajo con los sistemas de información por parte de los empleados.
- Un alto porcentaje de este grupo empresarial invierte poco en entrenamiento y capacitación para el personal encargado de la plataforma informática.

- Las empresas estudiadas utilizan frecuentemente protección de antivirus y firewalls, lo cual es indicativo de que le sector se mantiene al día con algunos de los avances en tecnologías de la información.
- Se encontró que en la muestra estudiada las herramientas para monitorear o rastrear redes de computadoras o sistemas de información, no son de uso tan común dentro de este grupo empresarial.
- Una alta proporción de las PyME's, audita sus sistemas con relativa frecuencia, y otro porcentaje de estas empresas investigadas, verifican la confiabilidad en el procesamiento de datos y los problemas que ocurren dentro de su plataforma informática.
- En lo que corresponde al marco legal que establece nuestro país para la información y sobre los conocimientos del estándar ISO-17799, para la preservación de la información, la mayoría de las PyME's consultadas, manifestó no conocer dicha normativa.

Recomendaciones

De acuerdo con uno de los objetivos propuestos en la investigación, se plantean las siguientes sugerencias, tomando como base el estándar ISO-17799 para la seguridad de la información, sustentándose en los resultados obtenidos.

- En lo referido a las políticas de seguridad de la información, es necesario que asuman estas con mayor intensidad y que además se establezca un plan de difusión a todos los miembros de la organización, para lograr alinearlas con los objetivos principales del negocio.
- Es necesario que las PyME's conozcan el estándar ISO-17799 diseñado para la preservación de la información en los sistemas de información, el cual puede adaptarse a esta en forma progresiva.

- Para la adopción de la norma ISO-17799, puede realizarse la participación en talleres o cursos que permitan conocer el funcionamiento de la norma y posterior difusión a los miembros de la organización.
- Las empresas PyME’s pueden mejorar la calidad del recurso humano dedicado al aseguramiento de la información, mediante entrenamiento, asistencia a cursos, congresos o seminarios, que les proporcionen las técnicas de vanguardia que pueden aplicarse para incrementar la seguridad de la información en las PyME’s.
- Todo el personal de una empresa PyME, debe conocer sus funciones, permisos de acceso a la información y responsabilidades sobre los activos de la información, de acuerdo con el cargo que desempeñan en la empresa.
- Los activos de la información, deben identificarse y clasificarse de acuerdo con su relevancia, además asignar el personal responsable de su administración sobre todo para los que están asociados con los procesos vitales de la empresa, como por ejemplo el proceso de facturación.
- En cuanto a la seguridad física y ambiental, las PyME’s necesitan ir cambiando de forma gradual de los controles mas comunes a nuevos medios de aseguramiento del perímetro empresarial, que garanticen, que los activos tanto empresariales, así como los de la información, estén debidamente protegidos.
- Para el control de los sistemas de información y redes de computadoras, las PyME’s deben concentrar sus esfuerzos, ayudándose con herramientas disponibles en el mercado para esta tarea, algunas de las cuales se basan en software libre que no resultarían complejas y costosas al momento de instalarlas.
- Es necesario que dentro de la normativa empresarial se incluyan medidas de seguridad para prevenir errores o problemas dentro de los sistemas de información, instalando procesos de auditoria y verificación de la información manejada a través de los sistemas.

- Establecer en el plan de continuidad del negocio los pasos a seguir, en caso de que se presenten problemas en la plataforma informática, que afecten el desempeño regular de los sistemas de información que estén en funcionamiento, tarea que debe involucrar a la gerencia de las PyME's.
- En el cumplimiento con la normativa jurídica venezolana para la seguridad de la información, este grupo empresarial necesita documentarse a un más, lo que se puede hacer a través de seminarios o talleres o con empresas consultoras que prestan este servicio.

Lineamientos propuestos mejorar para la seguridad de información en las PyME's, los cuales tienen como referencia el estándar ISO-17799 para la seguridad de la información:

1) La gerencia de las empresas PyME's, necesitan incluir dentro de sus planes administrativos, la seguridad de los activos de la información, indicando cual es la información más valiosa para su organización y que debería protegerse. Una vez hecha la normativa, esta debe ser del conocimiento de toda la empresa. El documento debería revisarse periódicamente para evaluar su funcionamiento y agregar las modificaciones que fueran necesarias
2) Las empresas a través del personal encargado de administrar los sistemas, deben definir las responsabilidades de los usuarios, dentro de los sistemas de información, las cuales pueden ser explicados por medio de talleres o charlas con el personal objetivo.
3) Es importante que la gerencia junto con el personal de sistemas, identifiquen y clasifiquen los activos de la información, que pueden ser elementos de hardware, software, bases de datos, redes de computadoras, personas entre otros. Además de determinar su nivel de importancia para el buen funcionamiento de los sistemas de información que apoyan las operaciones de una PyME.

4) El trabajo de los usuarios con los sistemas de información debe ser supervisado, para identificar errores en la información procesada o el mal uso de los activos de la información por parte de los mismos. Explicar a los usuarios la importancia que tiene la información para la empresa, cuales son las amenazas a las que esta expuesta y cuales son las vulnerabilidades o riesgos que puede afectarla, además de que pueden informar sobre problemas encontrados en el tratamiento de la misma.

5) Las instalaciones físicas o locales donde están las computadoras que dan soporte al funcionamiento de los sistemas de información, deben contar con niveles de protección de acuerdo a su importancia o criticidad, establecer controles de acceso de forma tal, que en esta área sólo estén las personas autorizadas. Asegurar los locales frente a riesgos factibles como puede ser hurto tanto de equipos como de información, incendios o cualquier otro percance que pudiera ocurrir.

6) La empresa debe asegurarse de la operación adecuada y protegida de los recursos de la información, para lo cual necesita tratar de reducir los riesgos que afectan el funcionamiento de los sistemas de información, esto se puede lograr controlando la instalación de hardware, software, chequeando la disponibilidad de los servicios de la información, atendiendo y monitoreando el funcionamiento de las redes de datos, reducir los daños o interrupciones en los servicios de la información, atender prontamente cualquier anomalía que se presente. Esto con el objetivo de asegurar que los servicios de los sistemas de información siempre estén disponibles, evitando interrupciones o daños en el funcionamiento operativo de la empresa.

7) En lo relativo a los accesos, cada usuario debe tener establecido sus privilegios de acceso para las aplicaciones, sistemas de información, Internet, sistemas operativos, etc. Los servicios de la información deben rechazar a todos aquellos usuarios que no cumplan con los requisitos de acceso; las entradas no autorizadas, así como los intentos fallidos de acceso a sistemas deben ser investigados. Si existe acceso externo a los sistemas de

información de la empresa, estos deben estar garantizados a través de herramientas de red o controles específicos para el área.

8) Si la empresa compra o encarga el desarrollo de los sistemas de información que utiliza para el desempeño de sus operaciones, estos deben incluir procedimientos de seguridad que permitan conservar la integridad y autenticidad de los datos que manejan, estos procedimientos deben cubrir todos los módulos y con diferentes niveles de acceso. La seguridad de la información cubre todas las etapas en el desarrollo de un sistema, además deben usarse los acuerdos de confidencialidad con desarrolladores o proveedores de software.

9) El plan de continuidad del negocio o de contingencia debe contener las actividades y el personal responsable que es necesario, para que la empresa sigua funcionando en caso de problemas graves, sobre todo si estos se relacionan con los sistemas de información.

10) El proceso de seguridad de la información, busca asegurar que esta cumpla con las normas legales o jurídicas que tiene cada país para su manejo o tratamiento. Las empresas deben revisar la normativa jurídica vigente, que se refiera al tratamiento de la información e integrarla a las políticas de seguridad de la información empresariales. Es necesario que se implemente planes de auditoria interna en cada empresa, lo cual es una forma para detectar problemas dentro de los sistemas de información, que además permitan aplicar los correctivos necesarios y que se adapten a las normas legales del país.

Para concluir se presenta en la figura Nro. 10, un esquema sobre los pasos a seguir por la PyME, para mejorar la seguridad de la información en sus sistemas.

Figura 10: Esquema para la seguridad de la información en la PyME.
Fuente: Elaboración propia, Villasmil (2006).

REFERENCIAS BIBLIOGRÁFICAS

Anteproyecto de Ley de Tecnologías de la Información, Versión (05/08/2005). República Bolivariana de Venezuela, (2001), Ministerio de Ciencia y Tecnología. (Doc. Pdf)

BALESTRINI, M., (1997). **Como se Elabora el Proyecto de Investigación.** BL Consultores Asociados. Caracas.

BARZANALLANA, R., (2006). **La Seguridad en Informática. Apuntes docentes.** Universidad de Murcia, España. Url. http://www.um.es/docencia/barzana/IAGP/Iagp10.html. Consulta (20/05/2006).

BERBESI, L., (2005). **Caracterizando a la Pyme en Venezuela**. Conferencia. Fundes. Url. www.consecomercio.org.ve/Ponencias_Asamblea2005/Libia_Berbesi_FUNDES_Asamblea2005.pps Consulta (22/02/2006)

BORGHELLO, C., (2001), **Seguridad Informática: sus implicancias e implementación.** Trabajo de Grado. Universidad Tecnológica Nacional de Argentina. Url:http://www.htmlweb.net/seguridad/tesis/tesis.html. Consulta (04/04/2006)

BOSSIO, H., y GROS, C., (2003). **Seguridad Informática parte de la Cultura del Control**. Conferencia. Consejo Profesional en Ciencias Informáticas. Argentina. Url: www.cpci.org.ar/newsletters/91/conferenciaseguridad.pdf. Consulta (04/04/2006)

BRITO, X., DIAZ, Y., VALERA, J., (2001). **Casos Simulados de Redes Empresariales entre Pequeñas y Medianas Empresas**. Trabajo de Grado. Universidad Centroccidental Lisandro Alvarado, Decanato de Administración y Contaduría, (Barquisimeto).

CÓRDOVA, N., (2003). **Plan de Seguridad Informática para una Entidad Financiera.** Trabajo de Grado. Universidad Nacional Mayor de San Marcos. Facultad de Ciencias Matemáticas. EAP de Computación. Lima, Perú. Url: http://sisbib.unmsm.edu.pe/bibvirtual/Tesis/Basic/cordova_rn/contenido.htm. Consulta (11/04/2006)

DONADO, S., AGREDO, G., CARRASCAL, C., (2002). **Políticas de Seguridad Computacional**. Facultad de Ingeniería Electrónica y Telecomunicaciones, Universidad del Cauca – Colombia. Url: http://www.criptored.upm.es/guiateoria/gt_m124c.htm Consulta (18/04/2006)

El portal de ISO 27000 en español. **Sistema de Gestión de la Seguridad de la Información.** Url: http://www.iso27000.es/sgsi.html, http://www.iso27000.es/iso27000.html**,** Consulta (26/04/2006)

ESPIÑEIRA, SHELDON Y ASOCIADOS, (2005). **Seguridad de la Información: Un nuevo enfoque para el control de riesgos de negocio.** Articulo. Url: www.pc-news.com/detalle.asp?sid=&id=11&Ida=1926. Consulta (25/04/2006)

GAXIOLA, J., (2004). **Tecnologías de Información para las Pymes**. Instituto Tecnológico de Sonora Área de Tecnología de Información y Comunicaciones. Articulo. Url. http://www.gestiopolis.com/canales5/emp/pymecommx/52.htm. Consulta (01/02/2006)

HERNÁNDEZ, R., FERNÁNDEZ, C., BAPTISTA, P., (2004). **Metodología de la Investigación**. 3era. Edic. McGraw Hill.

HERNANDO, S., (2005). **El coste de los problemas de seguridad**. Hispasec Sistemas. F/Publicación. 01/08/2005. Url: www.hispasec.com/unaaldia/2473 Consulta (23/02/2006).

ITELLIGENCE DE VENEZUELA, (2005). **Políticas de Seguridad Informática: Mejores Prácticas Internacionales.** Conferencia. Url: http://www.cavedatos.org.ve/download/cdt_289.pps Consulta (25/04/2006)

IZQUIERDO, F., (2005). **Administración de Riesgos de TI.** Conferencia**.** Banco de la República de Colombia**.** Url: www.felaban.com/memorias_congreso_clain_2005/ 10izquierdo_f_adm_riesgo_ti.pdf. Consulta (24/04/06)

JIMENEZ, J., (2005). **Evaluación seguridad de un sistema de información.** Perú: Ilustrados.com, 2005. (p 10 – 19). Url: http://site.ebrary.com/lib/biblioelectronucla/Doc?id=10095478&ppg=10 Consulta (11/04/2006). Base de Datos E-Libro.

LAUNDON, K. y LAUNDON, J., (2002), **Sistemas de Información Gerencial,** 6ta Edic. Editorial Prentice Hall.

LEDÓN, P., (2005). **Las Tecnologías de Información para las PyME's, Revolución que no tiene Reversa.** Instituto Tecnológico y de Estudios Superiores de Monterrey Campus Guadalajara. Articulo Url. http://www.gestiopolis.com/canales2/gerencia/1/tipymes.htm. Consulta (10/01/2006)

Ley Especial Contra Delitos Informáticos, República Bolivariana de Venezuela, (2001), Gaceta Oficial Nº 37.313. http://www.mct.gov.ve/leyes/lsdi.htm. consulta (03/02/2006)

Ley Orgánica de Telecomunicaciones, República Bolivariana de Venezuela, (2000), Gaceta Oficial Nº 36.920. http://www.mct.gov.ve/leyes/lote.htm. consulta (03/02/2006)

Ley para la Promoción de la Pequeña y Mediana Industria. República Bolivariana de Venezuela, (2002). Gaceta Nº 37583 del 03-12-2002. Url. www.mpd.gov.ve/decretos_leyes/Leyes/ley_para_la_promocion_y_desarrollo_de_la_pequena_y_mediana_industria.pdf

Ley Sobre Mensajes De Datos Y Firmas Electrónicas, República Bolivariana de Venezuela, (2001), Decreto con Fuerza de Ley. http://www.tsj.gov.ve/legislacion/dmdfe.htm

Ley Sobre Mensajes De Datos Y Firmas Electrónicas, República Bolivariana de Venezuela, (2001). Consulta (03/02/2006)

LIZAMA, J., y FARIAS, M., (2003). **Analfabetismo Digital y sus Implicancias en la Seguridad Informática.** Articulo. Universidad Nacional Autónoma de México. Url: http://www.criptored.upm.es/guiateoria/gt_m217c.htm. Consulta (03/04/2006)

MENDOZA, E., (2005). **Impacto de la Tecnología de Información en la Competitividad de las Pequeñas y Medianas Industrias.** Trabajo de Postgrado. Universidad Centroccidental Lisandro Alvarado. Decanato de Administración y Contaduría, (Barquisimeto).

Ministerio de administraciones publicas de España, Consejo Superior de Informática. **Guías técnicas de Seguridad de los Sistemas de Información**. (2001). Url: http://www.csi.map.es/csi/silice/homepage.html. (Consulta 23/02/2006)

MORA, C., (2004). **Debilidades de la PyME's Venezolanas. PyME's y Recursos Humanos. PyME's y Tecnología.** Estudios de Postgrado de

la Universidad de Carabobo. Articulos. Url. http://www.gestiopolis.com/Canales4/emp/devepymes.htm. Consulta (29/04/2006)

O'BRIEN, J., (2001), **Sistemas de Información Gerencial,** 4ta Edic. Editorial McGraw Hill, Colombia.

OLIVARES, J., (2005). **Actualización ISO/17799:2005(E).** Conferencia. Consultura Neosecure. Url. http://cibsi05.inf.utfsm.cl/trabajos.htm Consulta (04/04/2006)

OZ, E., (2001), **Administración de Sistemas de Información,** 2da Edic. Editorial Thomson Learning DF. México.

Plan Nacional de Tecnologías de la Información, República Bolivariana de Venezuela, (2001), Ministerio de Ciencia y Tecnología. Url. http://www.cnti.ve/cnti_docmgr/sharedfiles/PlanNacionaldeTI.pdf. consulta (03/02/2006)

RAMIÓ, J., (2003). **Aspectos Comparativos de la Seguridad Informática entre España y Latinoamérica**. Ponencia. 2do Congreso Iberoamericano de Seguridad Informática. Colombia. Url: http://www.criptored.upm.es/guiateoria/gt_m001f.htm consulta (22/02/2006)

RAMIÓ, J., (2006**). Libro Electrónico de Seguridad Informática**. Versión 4.1. Universidad Politécnica de Madrid. Url: http://www.criptored.upm.es/guiateoria/gt_m001a.htm Consulta (10/04/2006)

SABINO, C., (1992). **El Proceso de la Investigación**. Editorial Panapo Caracas.

SENA, L., TENZER, S., (2004). **Introducción al Riesgo Informático.** Cátedra de Introducción a la Computación. Facultad de Ciencias Económicas y de Administración Universidad de la República, Uruguay. Url. www.tenzer.com.uy/archivos/riesgoinf8.pdf Consulta (14/04/2006)

TORRES, J., (2003). **Políticas de Seguridad Informática.** Director de Tecnología e Información Scientech de Venezuela. Articulo. Url. www.pc-news.com/detalle.asp?sid=&id=11&Ida=1255. Consulta (27/06/2006)

VILLALON, A., (2004). **Código de Buenas Prácticas de Seguridad UNE-ISO/IEC 17799**. Valencia – España. url. http://www.criptored.upm.es/guiateoria/gt_m209d.htm consulta (24/02/2006)

VILLALON, A., (2005). **Seguridad de los Sistemas de Información.** Grupo S2. España.
Sistema de Gestión de la Seguridad de la información: Calidad de la Seguridad. Conferencia. Grupo S2. España**.** Url: http://www.criptored.upm.es/guiateoria/gt_m209f.htm Consulta (18/04/2006).

WITTE, E., (2003). **Sensibilización en Seguridad Informática.** Conferencia. ArCERT. Argentina. Url: www.arcert.gov.ar/cursos/curso_sensibilizacion/sensibilizacion-seg-inf.ppt. o www.arcert.gov.ar Consulta (26/04/2006)

ANEXO B

.-*Instrumento de Recolección de Datos*

UNIVERSIDAD CENTROCCIDENTAL
"LISANDRO ALVARADO"
DECANATO DE CIENCIAS Y TECNOLOGÍA
COORDINACIÓN DE POSTGRADO

Estimado(a):

La presente encuesta, se ha diseñado con el objetivo de analizar los riesgos de seguridad informática que pueden afectar a una empresa. Mediante éste instrumento se recolectará la información necesaria para satisfacer los planteamientos de la investigación, la cual corresponde al trabajo de grado para la "Especialización en Tecnologías de la Información y Comunicaciones", de la Universidad Centroccidental "Lisandro Alvarado", la cual se denomina "*Análisis de los Riesgos de Seguridad Informática, para las Pequeñas y Medianas Empresas (PyME's) usando el estándar ISO-17799, para la definición de políticas de seguridad que protejan sus Sistemas de Información"*. Por tanto agradezco su valiosa colaboración y su disposición para el llenado de la encuesta, apreciando su objetividad al momento de responderla.

Toda la información recolectada, es de absoluta confidencialidad y el trato que se le dará a la misma, será sólo con fines académicos, por lo que no es necesaria su identificación.

Gracias, por su valiosa ayuda.

Atentamente,

AdS. Fabiola Villasmil

INSTRUMENTO DE RECOLECCIÓN DE DATOS

Instrucciones para el llenado:

Lea detenidamente cada proposición, luego según su criterio, marque con una equis (X), la alternativa de su preferencia. No deje proposiciones sin responder.

1) ¿Se han adoptado políticas de seguridad para la protección de los equipos de computación y de la información en la empresa?

☐ Si ☐ No

2) ¿La empresa posee Manuales de normas y procedimientos que indiquen?

☐ Uso de los equipos de computación de la empresa

☐ Uso de los sistemas de Información de la empresa

☐ Los permisos y restricciones para acceso a la información

☐ El personal que tiene derecho de acceso a los computadores

☐ El horario para accesar o trabajar con los computadores

☐ No tienen manuales para el área de sistemas

3) ¿La empresa dispone de un inventario actualizado de todos los equipos de computación, aplicaciones de software y de su respectiva ubicación?

☐ Si ☐ No

4) ¿Existe personal encargado de la seguridad de la información dentro de la empresa?

☐ Si ☐ No

5) ¿Las personas encargadas de la administración de los sistemas de información, se capacitan con frecuencia?

☐Siempre ☐casi siempre ☐ a veces ☐nunca

6) ¿Existen acuerdos de confidencialidad sobre la información, con empleados y terceros?

☐Siempre ☐casi siempre ☐ a veces ☐nunca

7) ¿La planta física donde están las computadoras, está libre de riesgos como?

- ☐ Inundaciones
- ☐ Terremotos
- ☐ Fuego
- ☐ Sabotaje
- ☐ Otros(indique)_____

8) ¿Los locales donde están las computadoras poseen?

- ☐ Aire acondicionado
- ☐ Alarmas contra fuego
- ☐ Detectores de Humo
- ☐ cerraduras especiales
- ☐ Otros(indique) _____

9) ¿El acceso de personas a la empresa es controlado por?

- ☐Circuito cerrado de TV
- ☐Control de acceso por medios electrónicos
- ☐Vigilancia solo en la entrada principal
- ☐ Otro(indique)_____

10) ¿Existen baterías o UPS para resguardo de los computadores importantes de la empresa?

☐ Si ☐ No

11) ¿Se respaldan los archivos o bases de datos?

☐Siempre ☐casi siempre ☐ a veces ☐nunca

12) ¿Se actualiza la plataforma de Software usado en la empresa (sistemas operativos, paquetes de oficina, antivirus, software de redes entre otros)?

☐Siempre ☐casi siempre ☐ a veces ☐nunca

13) ¿Se utilizan firewalls para controlar el acceso externo a los computadores de la empresa?

☐ Si ☐ No

14) ¿Se tienen herramientas para el monitoreo de sistemas y de la red de computadoras?

☐Siempre ☐casi siempre ☐ a veces ☐nunca

15) ¿Se verifica la confiabilidad del procesamiento de datos en los sistemas de información?

☐Siempre ☐casi siempre ☐ a veces ☐nunca

16) ¿Se cambian las claves de acceso (pass Word)?

☐Siempre ☐casi siempre ☐ a veces ☐nunca

17) ¿Todos los usuarios de los equipos de computación tienen acceso a Internet?

☐Siempre ☐casi siempre ☐ a veces ☐nunca

18) ¿Los sistemas de información tienen incluidos procedimientos para la seguridad de la información?

☐Siempre ☐casi siempre ☐ a veces ☐nunca

19) ¿Se detectan rápidamente los problemas ocurridos dentro de la plataforma informática de la empresa?

☐Siempre ☐casi siempre ☐ a veces ☐nunca

20) ¿Se auditan los sistemas de información?

☐Siempre ☐casi siempre ☐ a veces ☐nunca

21) ¿La empresa tiene un plan de recuperación en caso de desastres, que permita la continuidad del negocio?

☐ Si ☐ No

22) ¿La empresa adquiere pólizas de seguros para los equipos de computación?

☐Siempre ☐casi siempre ☐ a veces ☐nunca

23) ¿Se conocen las Normas ISO-17799 para la seguridad de la información?

☐ Si ☐ No

24) ¿Se conoce la normativa jurídica venezolana para la protección de la información?

☐ Si ☐ No

ANEXO C

.-*Validación del Instrumento de Recolección de datos por Juicio de Expertos.*

UNIVERSIDAD CENTROCCIDENTAL
"LISANDRO ALVARADO"
DECANATO DE CIENCIAS Y TECNOLOGÍA
COORDINACIÓN DE POSTGRADO

Estimado Profesor(a):

Me dirijo a usted cordialmente, con el objetivo de solicitar su valiosa colaboración para medir la validez del instrumento de recolección de datos (anexo). El mismo se elaboro con el propósito de recopilar la información acerca de la investigación: *"Análisis de los Riesgos de Seguridad Informática en las Pequeñas y Medianas Empresas (PyME's), usando el Estándar ISO-17799 para la definición de políticas de seguridad que protejan sus Sistemas de Información"*, la cual corresponde al trabajo de grado para la **"***Especialización en Tecnologías de la Información y Comunicaciones",* de la Universidad Centroccidental "Lisandro Alvarado". El instrumento permitirá recolectar la información necesaria para satisfacer los objetivos de la investigación. Su misión en la validación, consistirá en verificar la consistencia, coherencia de los indicadores y su relación con los planteamientos de la investigación, desde el punto de vista temático así como metodológico. Por tanto agradezco su conveniente aporte al referido instrumento.

Gracias, por su valiosa ayuda.

Atentamente,

AdS. Fabiola Villasmil

UNIVERSIDAD CENTROCCIDENTAL
"LISANDRO ALVARADO"
DECANATO DE CIENCIAS Y TECNOLOGÍA
COORDINACIÓN DE POSTGRADO

MATRIZ DE VALIDACIÓN PARA JUICIO DE EXPERTOS

Indicador Información sobre:	**Ítems**	**Apreciación**			
		A	**B**	**C**	**D**
◆ Sistemas y software en uso en la empresa	12,13,14				
◆ Permisos para acceso a la información	2,17,18				
◆ Normas para el uso de la información y equipos de computación	1,2,6,16				
◆ Normas para el respaldo de datos	2, 11				
◆ Conocimiento de las norma jurídicas para el uso de la información	24				
◆ Pólizas de seguros	22				
◆ Control de acceso y seguridad física de las instalaciones de la empresa	7,8,9				
◆ Uso de Firewalls	13				
◆ Uso de Antivirus	12				
◆ Control de acceso a sistemas de información	15,16,17,18				
◆ Políticas de seguridad documentadas para el uso de la información	1,2,19,20				
◆ Conocimiento de la norma ISO-17799	23				
◆ Asignación de responsabilidades en materia de seguridad de la información.	4,5				

Referencia:

A = Dejar **B** = Modificar **C** = Eliminar **D** = Incluir otra pregunta

Observaciones:_____
_____
_____
_____
_____
_____