Universidad de las Ciencias Informáticas
Facultad 3

Trabajo de Diploma para optar por el título de Ingeniero en ciencias Informáticas

Título: Propuesta de Plan de Seguridad Informática para la Empresa PDVAL

Autor: Juan Carlos Navarro Carrión

Tutor: Ing. Vlamir Rodríguez Fernández

Junio 2009

DECLARACION DE AUTORIA

Declaro que soy el único autor de este trabajo y autorizo a la Facultad 3 de la Universidad de las Ciencias Informáticas a hacer uso del mismo en su beneficio.

Para que así conste firmo la presente a los ____ días del mes de _____ del año _____.

Juan Carlos Navarro Carrión

_____

Firma de Autor

Ing. Vlamir Rodríguez Fernández

_____

Firma de Tutor

AGRADECIMIENTOS

A mis padres por haber trabajado conmigo en la tesis, por todo el apoyo y ánimos dado a lo largo de mi existencia, por enseñarme el camino ha convertirme en un hombre del que estén orgullosos.

A mi hermana Maribella por su ayuda y apoyo para que la tesis avanzara.

A mis tíos Maribel y Morejón y mis primos Rigo e Hidelmaris, por toda la ayuda y la atención prestada durante toda mi carrera.

A mi novia Daylin por todos sus consejos y haber estado siempre presente para mí.

A mi tutor Ing. Vlamir Rodríguez Fernández, por su preocupación, su exigencia en el cumplimiento del trabajo y ser un buen amigo.

Al Ing. Dusniel Horta Centeno por el apoyo, preocupación y guía en mi trabajo.

A los compañeros de mis padres Lender y Yusmany por toda la documentación facilitada.

A mis padres, por su apoyo y por creer en su hijo, a mis hermanas, y especialmente a mi tía Maribel por toda la ayuda durante toda mi carrera.

RESUMEN

La importancia que ha tomado en la actualidad el aseguramiento de la información en las organizaciones, debido al alto valor que representa este activo, estas últimas han comenzado a prestar especial interés en este sentido, como una vía de asegurar la supervivencia o competitividad. En el presente trabajo se realiza una investigación de las metodologías y mejores prácticas sobre el proceso de confección de planes de seguridad informática; además de desarrollar una propuesta de plan de seguridad informática para la empresa venezolana PDVAL (Productora y Distribuidora Venezolana de Alimentos). En el cual se propone una plantilla de elaboración de planes de seguridad y estructuras de gestión y control de la seguridad informática para dicha empresa; ya que la misma no cuenta con un plan se seguridad concreto ni una estructura oficial dentro de la empresa dedicada a este tipo de actividades en la misma.

INTRODUCCION

La empresa PDVAL surge como una estrategia del gobierno bolivariano en respuesta a un fenómeno que se estaba dando en Venezuela relacionado con la distribución de alimentos a la población; el acaparamiento, contrabando y desvío de productos por parte de las empresas privadas dedicadas a la distribución y venta de alimentos. Debido a este problema surge PDVAL, con el objetivo de erradicar esa situación y brindar una fuente estable de alimentos y a precios regulados; que en un inicio se pensó solamente en alimentos de la canasta básica, pero actualmente incluye productos de la línea blanca, artículos electrodomésticos, de limpieza, aseo personal, etc. El gobierno a través de la empresa petrolera PDVSA (Petróleos de Venezuela S.A), ha habilitado por todo el territorio venezolano instalaciones como almacenes, plantas distribuidoras, procesadoras de granos y tiendas, estas últimas en dependencia del tamaño del inmueble son llamadas Híper-PDVAL o PDVAL.

Para el control y gestión de la empresa fue implantado un sistema informático de gestión empresarial, SENTAI. PDVAL surge como se dijo, bajo la tutela de PDVSA, el sistema está en funcionamiento sobre la infraestructura de la red informática de la empresa PDVSA, razón por la cual PDVAL no tiene su propia red, una solución rápida debido a la urgencia de que el proyecto saliera adelante inmediatamente. Debido a la premura el personal técnico inicial con que contó PDVAL pertenece a PDVSA integrantes del grupo de Automatización, Informática y Telecomunicaciones (AIT), con una organización prácticamente empírica, sin lineamientos, ni mecanismos establecidos que aseguren la protección de la información ni los activos informáticos. La empresa desde sus inicios ha presentado problemas en aspectos de comunicaciones, tráfico lento en la red, locales aislados del sistema temporalmente o en horarios críticos para el funcionamiento de la empresa, pérdida de documentación, extravío de mercancía, y muchas otras situaciones que afectan el funcionamiento de la empresa. En la práctica se ha comprobado que no existe orden en los departamentos de la misma, y falta de comunicación entre estos. Lo anteriormente dicho se refleja claramente, cuando una tienda no abre en tiempo, cuando hay que parar la venta con clientes dentro del local, para configuraciones de última hora, cuando las entidades de la empresa no envían la información pertinente en tiempo y retrasos acumulados y en aumento. Esto mancha evidentemente la imagen de la empresa, y PDVAL es un proyecto del gobierno, cualquier malfuncionamiento de la misma va más allá que un simple error empresarial debido a la situación política de ese país. De aquí la importancia que la empresa cuente con mecanismos bien establecidos que rijan la conducta laboral de la empresa y aseguren la protección de los activos e información de la empresa, para lograr que las nuevas instalaciones desde un inicio sean totalmente funcional y capacitadas para superar cualquier contingencia mediante planes

de acción ya escritos sin improvisaciones ante incidentes. Ya que uno de los objetivos de la empresa PDVAL además de la actividad comercial, es ser una fuente de empleo para los consejos comunales. Por lo que la formación y creación en el personal de una cultura de seguridad es de primer orden para poder establecer un buen funcionamiento de la empresa.

En correspondencia con lo planteado, será objetivo este trabajo dar solución al siguiente **problema:**

La ausencia de medidas y procedimientos que aseguren la seguridad de la información y los activos informáticos, así como la gestión de los mismos en la empresa PDVAL inciden negativamente en el cumplimiento de los objetivos de esta empresa. Por lo que el **objeto de estudio** de esta investigación será La Seguridad Informática, desarrollada sobre el **campo de acción** Gestión de Planes de Seguridad Informática. Por lo que si se logra confeccionar un plan de seguridad informática para la empresa PDVAL, el mismo influiría de forma positiva en el desempeño esta empresa.

Entonces, el **objetivo general** en este trabajo será desarrollar una propuesta de plan de seguridad informática para la empresa PDVAL. Desglosado en los siguientes **objetivos específicos**:

- Estudiar las normas y metodologías para la confección de Planes de Seguridad Informáticas.
- Realizar la propuesta de Plan de Seguridad Informática para la empresa PDVAL.
- Validar la propuesta de Plan.

Y para lograr el cumplimiento de los mismos se plantean las tareas investigativas siguientes:

- Investigación sobre temas de seguridad informática como conceptos, principios, seguridad lógica, seguridad física.
- Investigación sobre normas y metodologías para el desarrollo de Planes de Seguridad Informática.
- Estudio de métodos de análisis y estimación de riesgos
- Investigación sobre normas y metodologías sobre el desarrollo de Políticas de Seguridad Informática.
- Estudio de métodos para la elaboración de Planes de Contingencia Informática.

El trabajo esta estructurado de la siguiente forma:

Capitulo 1: Fundamentación teórica en el que se tratan temas esenciales relativos a la seguridad informática como conceptos, principios, metodologías y mejores prácticas para la realización de los planes de seguridad informática.

Capitulo 2: Propuesta de Plan se Seguridad Informática para la empresa PDVAL en el cual se desarrolla la propuesta de plan para esta empresa, en el mimo se utilizan los elementos investigados en el capitulo 1 y se hacen algunas propuestas y modificaciones a partir de los métodos estudiados.

Capítulo 3: Validación de la Propuesta de Plan de Seguridad Informática para la empresa PDVAL. En el capítulo se muestra el resultado obtenido producto a la encuesta aplicada a los expertos, la cual arrojo los resultados y la valoración sobre el plan propuesto.

1 CAPITULO 1: Fundamentación Teórica.

1.1 Introducción

En un mundo en el que el ordenador y el avance en la tecnología de la informática cobra cada vez más terreno, potenciado por el vertiginoso e importante crecimiento de la Internet, además de, la necesidad real de informatización y automatización de los procesos en un mundo cada vez más complejo, la empresa que no sea capaz de asegurar su red privada, que no tenga implantados procedimientos y métodos que garanticen la seguridad de su información y sus activos informáticos, ni sea capaz de reorganizarse y poner en marcha sus procesos tras un incidente de la seguridad, quedará en el camino, y la competencia en actual es implacable. El mundo informático es un terreno en el cual las conductas irresponsables y delictivas abundan y en algunos casos parecen incluso increíbles debido al alto desarrollo y capacidades cada vez más elevadas de los atacantes, el ciber-espacio lamentablemente ofrece un cierto grado de anonimato, lo que posibilita a los delincuentes cometer delitos tan comunes y antiguos como el robo, el fraude, la falsificación, entre otros, de formas muy sofisticadas. Se acostumbra desconocer o restar importancia al tema **seguridad informática** en las empresas. Y por esta razón, generalmente no se invierte en capital humano y financiero requerido para prevenir la pérdida o daño de la información; quizás por ser un sector que no genera ingresos, pero si protege las utilidades, ya que el activo más valioso con que pueda contar cualquier organización es la información y la infraestructura que la soporta. Durante el desarrollo de este capítulo se analizarán los principios, conceptos y metodologías del campo de la seguridad informática, en cuanto a la elaboración de planes de seguridad informática, su importancia, conceptos, estructura, estándares y metodologías para el desarrollo de los mismos.

1.2 Seguridad Informática

La información siempre ha sido un elemento clave en la existencia del hombre, es tan inofensiva como curiosidades en un libro para niños, letal como secretos militares en tiempos de guerras o valiosa, y sobre todo valiosa como para ser considerada un activo que posee una organización o empresa determinada, que tan solo el hecho de poseerla les brinda ventaja sobre las demás en el mercado. Por lo que es lógico que se piense en protegerla, entra aquí entonces la Seguridad Informática (SI), el pronunciar estas palabras nos dan una visión inmediata de lo que significan, pero realmente es algo mucho más que la idea inicial que se pueda tener. Según el sitio web de la Master Magazine la Seguridad Informática son "*técnicas desarrolladas para proteger los equipos informáticos individuales y conectados en una red frente a daños accidentales o intencionados.*"[1]. Otra definición de seguridad es presentada por ISO, en el que plantea *"La seguridad de la información es la protección de la información de un rango amplio de amenazas para poder asegurar la continuidad del negocio, minimizar el riesgo comercial y maximizar el retorno de las inversiones y las oportunidades comerciales."*[2]. La seguridad no se centra solamente en la información o en los equipos o soportes de la misma, este proceso, sin entrar en especificaciones, son estrategias desarrolladas a partir del análisis del entorno físico e informático en el que se desempeña una organización o entidad con el objetivo de proteger la información y todos los equipos y soportes en la que esta es procesada, por donde es transmitida y donde es almacenada, de cualquier daño accidental o predeterminado. Por lo que es algo más de lo que se pueda pensar, se reitera, ya que si se protegen solamente los equipos o soportes de la información, esta puede ser robada, modificada o destruida sin necesidad de tener acceso físico a los equipos que la soportan; y si de lo contrario se protege solamente la información mediante técnicas y configuraciones lógicas, entonces los equipos y lo soportes son los que pueden ser robados o destruidos. Es por eso que todo lo que represente una amenaza a la información desde cualquier punto de vista, relacionado con su integridad, confidencialidad y disponibilidad, es interés de la Seguridad Informática, ya que la misma se basa en estos principios para cumplir con sus objetivos.

[1] http://www.mastermagazine.info/termino
[2] Estándar ISO/IEC Internacional 17799, Segunda Edición 2005/06/15

1.2.1 Conceptos

Dato: Son símbolos, hechos que describen, situaciones, elementos o situaciones, los cuales son medibles y tienen la capacidad de asociarse a otros datos en un determinado contexto y generar información.

Información: Conjunto de datos, organizados significativamente que describen alguna situación, fenómeno o elemento.

1.2.2 Principios

La seguridad informática consiste en garantizar que el material y los recursos de software de una organización se usen únicamente para los propósitos para los que fueron creados y dentro del marco previsto. Esta por lo general se resume, en cinco objetivos principales:

- Integridad
- Confidencialidad
- Disponibilidad
- No repudio
- Autenticación

Aunque en ocasiones solo se tienen en cuneta los tres primeros, los cuales son principios básicos de la Seguridad Informática: la integridad, la confidencialidad y la disponibilidad.

1.2.2.1 La integridad

Según el diccionario de definiciones informáticas son "*Técnicas utilizadas para conseguir archivos de Back-up correctos de modo que se pueda recurrir a ellos en caso de tener que recuperar datos críticos después de que los datos originales se contaminen debido a una acción accidental o provocada (por ejemplo, un virus)*"[3]; la ISO 27001:2005 la define como "*Propiedad de salvaguardar la precisión y completitud de los recursos*"[4]. El principio define que la información deberá y será modificada solamente por los autorizados.

[3] http://www.asesoriainformatica.com/definiciones_i.htm
[4] http://www.delitosinformaticos.com/11/2006/seguridad-informatica/analisis-iso-270012005

1.2.2.2 La confidencialidad

Según la ISO 27001:2005, "*Propiedad que la información no esté disponible o pueda ser descubierta por usuarios no autorizados, entidades o procesos*" [5], el diccionario de definiciones informáticas la define como "*Calidad de secreto, que no puede ser revelado a terceros o personas no autorizadas*"[6]. Este principio garantiza que la información será legible solamente para los autorizados.

1.2.2.3 La Disponibilidad

La ISO 27001:2005 la define como "*Propiedad de ser accesible y usable bajo demanda por una entidad autorizada*"[7]. El principio asegura el acceso a la información solamente por los autorizados.

1.2.3 Seguridad Física

Cuando se habla de seguridad física, se hace referencia a todos aquellos mecanismos de prevención y detección para proteger físicamente los recursos del sistema; recursos como un simple teclado hasta un disco duro con el back-up de toda la información del sistema. Según el entorno y los sistemas a proteger esta seguridad será más o menos importante y restrictiva, aunque siempre deberemos tenerla en cuenta ya que es uno de los aspectos más olvidados a la hora del diseño de un sistema de medidas para asegurar la información en una organización.

1.2.3.1 Protección del hardware

El hardware es por lo general el elemento más caro de todo sistema informático y de ahí que las medidas para a asegurar su integridad son importantísimas en la seguridad física de cualquier organización. Y los problemas con los que comúnmente se suele lidiar son:

Desastres naturales: Estos pueden ser muy dañinos si la organización está expuesta a este tipo de amenaza y no se contempla en las medidas que se puedan tomar. Algunos desastres naturales a tener en cuenta:

[5] http://www.delitosinformaticos.com/11/2006/seguridad-informatica/analisis-iso-270012005
[6] http://www.asesoriainformatica.com/definiciones_i.htm
[7] http://www.delitosinformaticos.com/11/2006/seguridad-informatica/analisis-iso-270012005

- ✓ Terremotos y vibraciones
- ✓ Tormentas eléctricas
- ✓ Inundaciones y humedad
- ✓ Incendios y humos

Por lo que las medidas más comunes para este tipo de situaciones son:

- ✓ No situar equipos en sitios altos para evitar caídas.
- ✓ No colocar elementos móviles sobre los equipos para evitar que caigan sobre ellos.
- ✓ Separar los equipos de las ventanas para evitar que caigan por ellas o qué objetos lanzados desde el exterior los dañen.
- ✓ Utilizar fijaciones para elementos críticos.
- ✓ Colocar los equipos sobre plataformas de goma para que esta absorba las vibraciones.
- ✓ Uso de pararrayos.
- ✓ Desconectar los equipos antes de una tormenta.
- ✓ Indicadores de humedad.
- ✓ Sensores de calor y humo.

Acceso físico: Si el atacante tiene acceso físico a los equipos y soportes de la organización el resto de las medidas de seguridad implantadas resultan inútiles. Incluso, muchos ataques son tan triviales, como por ejemplo, la denegación de servicio por apagar la máquina que lo proporciona. Otros de los problemas que surgen a consecuencia de este son el robo de información y hardware. Para evitar todo este tipo de problemas se implantan mecanismos de prevención, controlar el acceso, y de detección, por si el mecanismo de prevención falla. En este sentido podemos contar con las soluciones siguientes en dependencia del nivel de de protección que desee la organización y si se justifican los costos:

- ✓ Analizadores de retina.
- ✓ Tarjetas inteligentes.
- ✓ Videocámaras.
- ✓ Vigilantes jurados.

1.2.3.2 Alteraciones del entorno

Hay que controlar problemas que puedan afectar el régimen de funcionamiento de las máquinas como la alimentación eléctrica, el ruido eléctrico o cambios bruscos de temperatura.

Electricidad: Los problemas relacionados con el sistema eléctrico que alimenta nuestros equipos quizás sean los más frecuentes; cortocircuitos, picos de tensión, cortes de flujo. Por lo que para la corrección de problemas como estos se instalan tomas de tierra o filtros reguladores de tensión, Sistemas de Alimentación Ininterrumpida (SAI). La electricidad estática es otra asesina de equipos electrónicos, por lo que se protegen con espráis antiestáticos o ionizadores, evitar tocar componentes metálicos, y que el ambiente esté excesivamente seco.

Ruido eléctrico: Generado por lo general por motores o maquinaria de alto consumo, también por ordenadores y otros equipos que existen en las oficinas, este se transmite a través del espacio o de líneas eléctricas cercanas a nuestra instalación. Por lo que las soluciones más sencilla es colocar el hardware lejos de los elementos que generen ruido, aunque de ser necesario se pueden instalar filtros, apantallar las cajas de los equipos o independizar el circuitos eléctrico de los equipos sensibles al ruido.

1.2.4 Seguridad Lógica

La información no sólo puede ser afectada de manera física si el hardware sufre algún daño, también informáticamente, a través de los programas de los mismos equipos que la almacenan, a través del mismo sistema implantado en la empresa o a través de la red informática de la misma. El activo más importante que pueda tener una organización es la información que se posee, y por lo tanto deben existir técnicas, más allá de la seguridad física, que la aseguren. Por lo que la seguridad lógica controla y salvaguarda la información generada por los sistemas, y por los programas en explotación, encargándose del control de acceso para mantener la integridad de la información protegiéndola de malos usos. Identifica individualmente a cada usuario y sus actividades en el sistema, restringe el acceso a datos, a programas de uso general y específico en las redes y terminales. Por lo que si esta es violada o es débil, entre las consecuencias encontraremos: alteración de datos en el momento de ingresarlos en el sistema o después, copia de programas y/o información, código oculto en los programas, virus informáticos, etc. Puede evitar la pérdida de registros, y ayuda a conocer el momento en que se produce un ataque a los sistemas.

1.2.4.1 Rutas de acceso

Los sistemas de información tienen ruta o rutas de acceso, las que se definen como trayectorias seguidas para el acceso al sistema, las cuales sirven para identificar los puntos de control que pueden ser usados para proteger los datos en el sistema.

1.2.4.2 Firewalls

El firewall es un filtro que protege los sistemas y las redes de una organización contra las conexiones inseguras o no deseadas, de esta forma se restringen el acceso a los recursos de la red desde un rango de direcciones IP, o direcciones MAC, determinadas por la dirección o administración de seguridad de la organización. Los firewalls los podemos encontrar en su variante hardware y software; la primera mucho más efectivos y seguros pero caros, y los segundos proveen ciertos niveles de seguridad y son mucho más baratos, incluso algunos sistemas operativos se instalan con un firewall de tipo software, como el del sistema operativo Windows. De forma general las configuraciones de los firewalls se basan en los siguientes tipos de paquetes de red:

- Los paquetes entrantes a la red.
- Los paquetes salientes de la red.
- Los paquetes en tránsito.

1.2.4.3 Protección contra programas dañinos

Es poco usual actualmente que las PC funcionen sin un producto antivirus instalado en las mismas, sobretodo para las que corren sobre versiones de Windows.

1.2.4.4 Claves de acceso

Esta es una de las áreas importante en la seguridad lógica, las claves de acceso de los usuarios son útiles para controlar el acceso a las computadoras, la información y los recursos de las redes, por lo que se restringe el uso de los mismos a los ajenos a las organizaciones, es una forma de identificar a los usuarios, saber quien hace, y que el administrador de la red en todo momento, conozca que actividad está en ejecución y que recursos están en uso, ya que atreves de las mismas se pueden definir niveles de acceso.

Las claves de acceso deben tener las siguientes características:

- El sistema debe verificar primero que el usuario tenga una clave de acceso válida.

- La clave de acceso debe ser de una longitud adecuada para ser un secreto.

- La clave de acceso no debe ser desplegada cuando es tecleada.

- Las claves de acceso deben ser encriptadas.

- Las claves de acceso deben de prohibir el uso de nombres, palabras o caracteres difíciles de retener, además las mismas no debe ser cambiadas por claves pasadas. Se recomienda la combinación de caracteres alfabéticos y numéricos.

1.2.4.5 Copias de seguridad

Es necesario establecer una política adecuada de copias de seguridad en cualquier organización; al igual que sucede con el resto de los equipos y software, los medios donde residen estas copias tendrán que estar protegidos físicamente; debido a que en una sola cinta o disco duro pueden haber copias de información contenida en varios servidores.

Lo primero es dónde se almacenan los dispositivos, donde se realizan las copias; un error común es almacenarlos en lugares cercanos a la sala de operaciones, cuando no en la misma sala; esto, que en principio puede parecer correcto (de hecho cómodo en caso de restaurar algunos archivos), puede convertirse en un problema serio si se produce cualquier tipo de desastre (ejemplo un incendio). Hay que pensar que generalmente el *hardware* se puede volver a comprar, pero una pérdida de información puede ser irreemplazable.

Así pues, lo más recomendable es guardar las copias en una zona alejada de la sala de operaciones; lo que se suele recomendar es disponer de varios niveles de copia, una que se almacena en una caja de seguridad en un lugar alejado y que se renueva con una periodicidad alta y otras de uso frecuente que se almacenan en lugares más cercanos y con menos procedimientos para su uso. Para proteger más aún, la información copiada se pueden emplear mecanismos de cifrado, de modo que la copia que guardamos no sirva de nada si no disponemos de la clave para recuperar los datos almacenados.

1.2.4.6 Soportes no electrónicos

Otro elemento importante en la protección de la información son los elementos no electrónicos que se emplean para almacenarla o transportarla, fundamentalmente el papel. Es importante que en las organizaciones que se maneje información confidencial se controlen los sistemas que permiten exportarla tanto en formato electrónico como en no electrónico (impresoras, plotters, faxes, teletipos).

Cualquier dispositivo por el que pueda salir información de nuestro sistema ha de estar situado en un lugar de acceso restringido; también es conveniente que sea de acceso restringido el lugar donde los usuarios recogen los documentos que lanzan a estos dispositivos.

Además de esto es recomendable disponer de trituradoras de papel para destruir todos los papeles o documentos que se quieran destruir, ya que evitaremos que un posible atacante pueda obtener información al revisar en la basura.

1.3 Plan de Seguridad Informática

El correcto funcionamiento de los sistemas de información es de vital importancia para los procesos que se desarrollan en una organización, debido a las facilidades de automatización que estos brindan y el hecho de contener informaciones valiosas de la misma, los convierte en objetos de ataques y accidentes. Los sistemas de información están expuestos a una gran cantidad de amenazas a causa de la propia vulnerabilidad de estos o a una incorrecta implantación de políticas, normativas para la seguridad, también una pobre o insuficiente inversión y capacitación del personal en este sentido. Para establecer un control en la identificación y tratamiento de situaciones en las que el sistema informático y la información de una organización se encuentren vulnerables ante ataques y accidentes, se elaboran los planes de seguridad informática. Un plan de seguridad informática es *"… la expresión gráfica del Sistema de Seguridad Informática diseñado y constituye el documento básico que establece los principios organizativos y funcionales de la actividad de Seguridad Informática en una Entidad y recoge claramente las políticas de seguridad y las responsabilidades de cada uno de los participantes en el proceso informático, así como las medidas y procedimientos que permitan prevenir, detectar y responder a las amenazas que gravitan sobre el mismo"*[8]. Por lo que los objetivos de los mismos son "*conocer el nivel de seguridad que presentan los sistemas informáticos, definir y diseñar el modelo de*

[8] MININT, Metodología para la elaboración del plan de seguridad informática

seguridad que se desea conseguir y planificar las acciones necesarias para ajustarse a ese modelo"[9]. En otras palabras los planes de seguridad informáticas no son más que los documentos que regirán la conducta laboral en una organización, en ellos se contempla el análisis de las situación actual en cuanto a seguridad de la entidad para la cual están diseñados, plantean la estructura que administrara los procesos de la seguridad en la organización a través de la políticas y estrategias para la preservación de la seguridad de la información y los activos informáticos.

1.3.1 Organización y estructura

En el apoyo bibliográfico sobre el cual se baso el autor para el desarrollo de este trabajo hace referencia a las normas ISO, para la elaboración de los planes de seguridad en particular la ISO-17799 la cual constituye buenas prácticas para el desarrollo de los mismos, las cuales no son pasos de estricto cumplimiento, sino que son adaptables y si el responsable por la elaboración de el plan decide obviar algunos pasos, en dependencia del tipo de entidad u organización a la que pertenezca, es totalmente normal y comprensible. La norma define a la seguridad como algo más que las medidas técnicas para la preservación de los principios de la seguridad informática, es además políticas y medidas organizativas, por lo que para alcanzar un buen plan de seguridad según la norma se deberán tener en cuenta los siguientes áreas de control:

1) Políticas de seguridad
2) Organización de la seguridad
3) Clasificación y control de activos
4) Seguridad del personal
5) Seguridad física y del entorno
6) Gestión de comunicaciones y operaciones
7) Control de accesos
8) Desarrollo y mantenimiento de sistemas
9) Gestión de la continuidad
10) Conformidad

Que cubrirán todo el ámbito de gestión de la seguridad, la misma cuenta además con 36 objetivos de control y 127 controles los cuales servirán para la validación del grado de adecuación a la norma, en el

[9]Guillermo B. Mora Marín, Directrices del Plan Director de Seguridad: ISO 17799

presente trabajo se utilizan algunas de las áreas de control propuestas por la norma y otras no, y algunas que son usadas en varios planes de seguridad de organizaciones nacionales y publicados en la internet, estudiados por el autor.

En el proceso de diseño de un Plan o Sistema de medidas para la Seguridad Informática se distinguen tres etapas:

1) Necesidades de protección del sistema informático:

   - ✓ Caracterización del sistema informático.
   - ✓ Identificación de amenazas y estimación de riesgos.
   - ✓ Evaluación del estado actual de la seguridad.

2) Definir sistema de medidas para la seguridad que garantice minimizar los riesgos identificados en la primera etapa.

   - ✓ Definir las políticas de seguridad.
   - ✓ Definir las medidas y procedimientos a implementar.

3) Evaluar el sistema de seguridad diseñado.

1.3.2 Gestión de riesgo

La gestión de riesgos en la que se sumergen las organizaciones ya sean privadas, públicas, gubernamentales o no, se ha convertido en un tema a considerar por la dirección de la organizaciones La gestión de riesgos, es el "*proceso sistemático de identificación y cuantificación de riesgos y la implementación de estrategias a fin de maximizar el valor de la organización*"[10]. La cual ha ganado importancia y consideración por parte de las direcciones de las empresas, ya que últimamente se habla y trabaja bajo el asecho de nuevos riesgos y más complejos. La antigua visión, de cuantificación de riesgos individualmente, sin análisis de relaciones y dependencias, a manera de elementos aislados, ha sido reemplazada por otra visión en la que se consideran los siguientes aspectos:

- Identificación y cuantificación de la mayor cantidad posible de riesgos,

[10] Carolina Cristina Castro, documento Gestión de riesgos y normas Argentinas.

- Los riesgos pueden impactar tanto en forma positiva (oportunidades) como negativa (amenazas) en los resultados de una organización.
- Existen relación entre riesgos y que interactúan entre sí.
- La dirección de las organizaciones debe estar involucrada en los procesos de gestión de riesgos.
- En toda organización es necesaria una visión de gestión de riesgos para maximizar las posibilidades de cumplir con los objetivos de la misma.

En este sentido internacionalmente, muchos organismos han realizado estudios y emitido estándares relacionados con la gestión de riesgos, tanto generales como específicos en determinado sector o industria, entre los que podemos mencionar: el Basilea II (para entidades financieras), el Solvencia II (para compañías de seguros, en estudio), COSO ERM (Enterprise Risk Management – Integrated Framework), AS/NZS 4360 (estándar australiano de gestión de riesgos, de uso general), la ISO 31000 y Guía 73 (Vocabulario) (proyecto de estándar internacional, y guía sobre vocabulario de gestión de riesgos), el PILAR, MGERIT, etc. En el caso particular de la metodología MAGERIT, la cual es una metodología española de gran aceptación y ampliamente usada en el proceso de análisis de riesgos, por lo que la misma será usada como guía para desarrollar el análisis de riesgos en este trabajo.

1.3.2.1 La metodología MAGERIT

Acrónimo de "Metodología de Análisis y GEstión de Riesgos de los Sistemas de Información de las AdminisTraciones Públicas". Es una metodología de carácter público elaborado por el Consejo superior de administración pública español. Es una metodología encaminada a conocer el riesgo al que está sometida una información y el grado de seguridad o inseguridad de la misma. Por lo que los objetivos principales de esta metodología son: hacer conciencia a los responsables de la información y de los sistemas, de la existencia de riesgos y la necesidad de administrarlos, ofrecer un método para el análisis de los mismos, ayuda a la elaboración de medidas que los mantengan controlados y brindarle a las organizaciones una preparación ante evaluaciones, auditorias, certificación, etc. La metodología está compuesta de 3 sub-modelos:

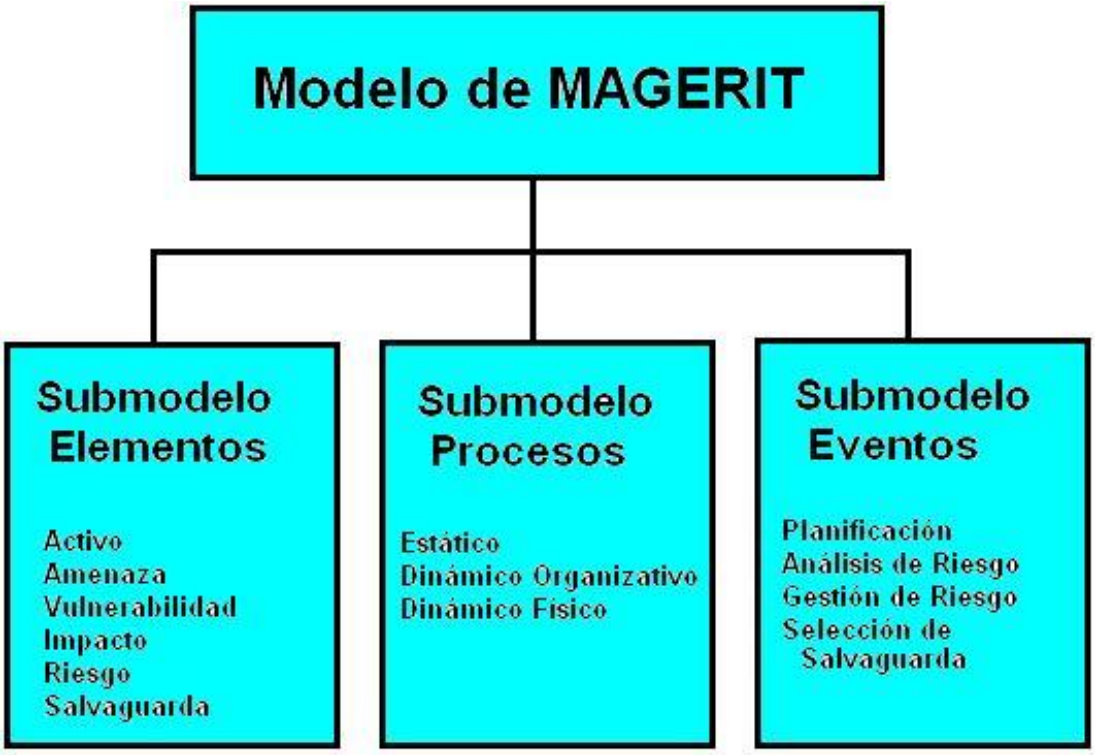


Figura 1. Sub-modelos de MAGERIT

Sub-modelo de Elementos

Lo componen los elementos siguientes:

Activo: es la meta del intruso o atacante, recurso del sistema informático o relacionado con este, necesario para que la organización y de mucho valor para esta, de este recurso informático o información puede depender el buen funcionamiento y/o el alcance de los objetivos de la organización.

Amenaza: situación, condiciones, elementos y todo aquello que represente la probable ocurrencia de un hecho que produzca daños materiales o no en los activos de una organización.

Vulnerabilidad: oportunidades a nivel de sistema y/o hardware que pueden ser explotadas por el atacante o intruso para hacer daño mediante un ataque.

Impacto: medición de las consecuencias de un daño al materializarse un ataque.

Riesgo: daño potencial que puede surgir por un proceso presente o evento futuro. Esta probabilidad de evento negativo tiene asociado un daño estimado conocido por la organización.

Salvaguarda: son las medidas que se puedan tomar, procedimientos y mecanismos para reducir el riesgo o el impacto de un incidente, esto incluye también las políticas de la seguridad.

Además de los elementos anteriores se deben tener en cuenta estos también:

Agente Hostil: persona o producto informático que perpetra un ataque o intento de ataque.

Ataque: acción exitosa o no, cuyo objetivo es causar un daño, robar información o utilizar un recurso informático de forma no autorizada.

Daño: consecuencia de una vulnerabilidad, materializada por un ataque.

Desastre: interrupción de la capacidad de acceso a información y procesamiento de la misma a través de computadoras necesarias para la operación normal de un negocio.

Sub-modelo de Eventos

Este modelo puede representarse como una “ciudad amurallada”, en la que los Activos son los habitantes y las Amenazas son el enemigo invasor. Las Salvaguardas son las murallas y sus brechas o grietas son las Vulnerabilidades. Entonces los Agentes Hostiles usan las Vulnerabilidades para producir un desastre y ocasionar Impactos en los Activos.

Vista estática del Sub-modelo de Eventos: refleja las relaciones generales entre los 6 elementos y se incluyen en esta vista los otros elementos mencionados para tener una mejor vista de la relación entre ellos.

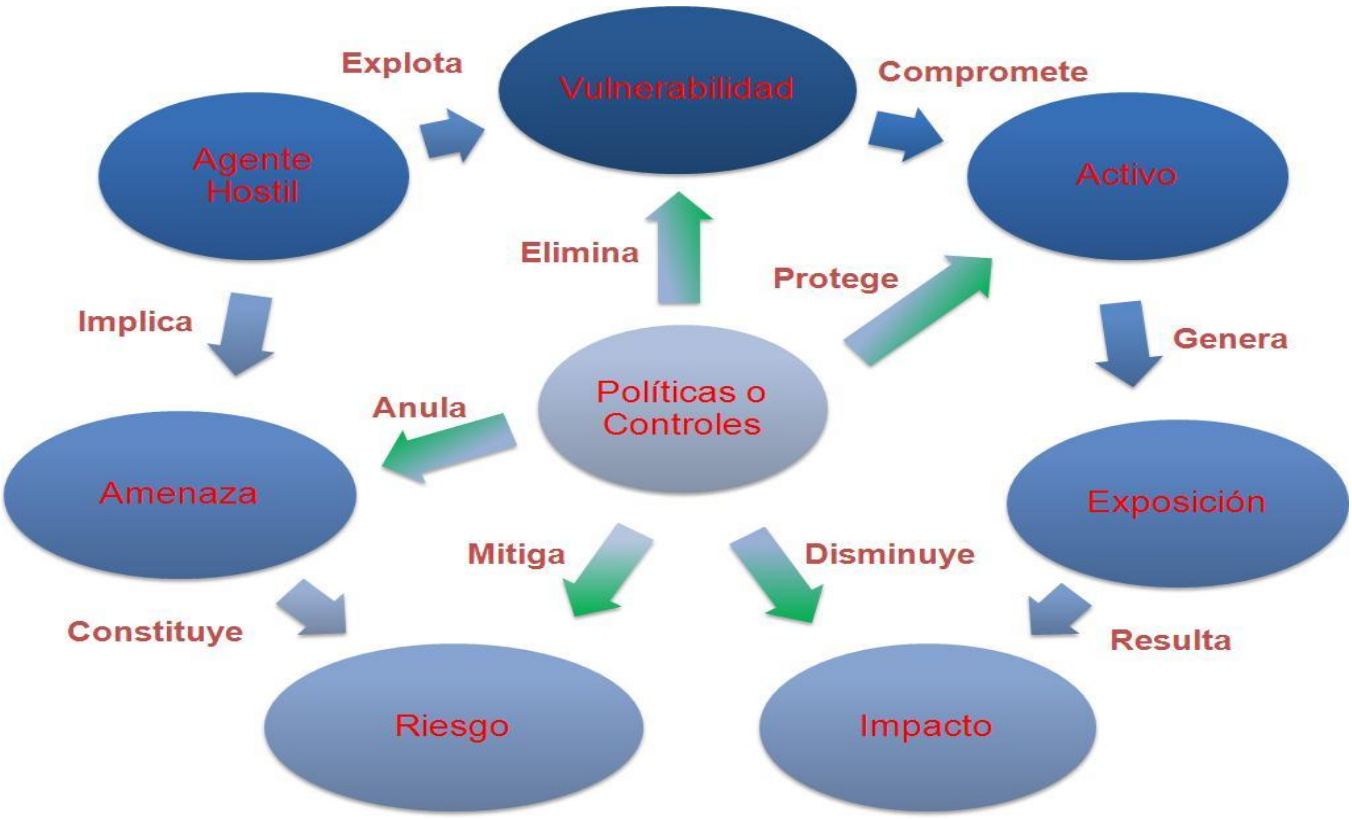


Figura 2. Relación de conceptos de la Gestión de Riesgo.

Vista dinámica organizativa del Sub-modelo de Eventos: recoge los 'escenarios' donde actúan los Elementos, esta vista articula las técnicas de cálculo de riesgos y selección de salvaguardas, la cual cuenta con dos sub-escenarios:

- **Sub-escenario de 'ataque':** coincide con el análisis de los riesgos y parte de la materialización de la amenaza (o agresión) a uno o varios tipos de Activos de la organización.
- **Sub-escenario de 'defensa':** coincide con la gestión de los riesgos y muestra cómo se pueden articular, frente a cada secuencia de 'ataque', las Salvaguardas apropiadas que funcionarán de una forma más o menos específica.

Sub-modelo de Procesos

El Sub-modelo de Procesos se divide en **etapas**, compuestas por **actividades** y éstas se desglosan en **tareas**.

Planificación del Proyecto de Riesgos: consideraciones iniciales para el proyecto de análisis y gestión de riesgos, se definen objetivos a cumplir y alcance, medios materiales y humanos llevarlo a cabo.

Análisis de riesgos: identificación y valoración de entidades, en la que se obtiene una evaluación del riesgo.

Gestión de riesgos: identificación de funciones y servicios de salvaguarda, para amortiguar los riesgos.

Selección de salvaguardas: prepara el plan de implantación de los mecanismos de salvaguarda elegidos y los procedimientos de seguimiento para la implantación.

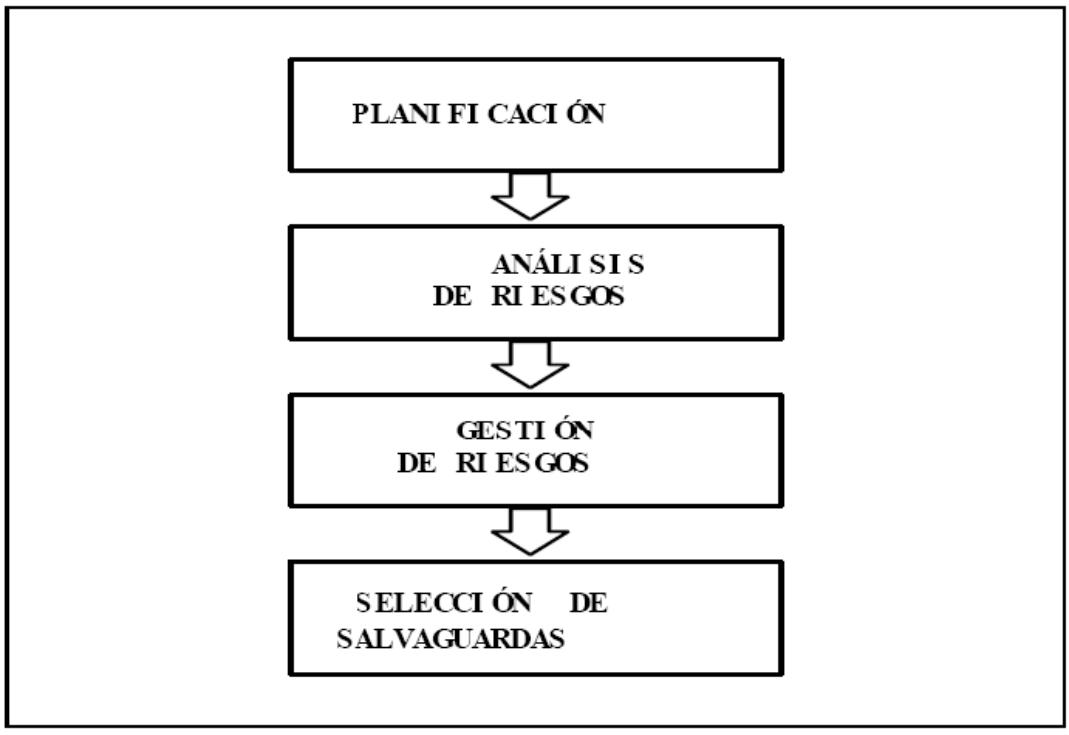


Figura 1. Sub-modelo de Proceso.

1.3.2.2 Que es lo que se protege

Toda organización debe tener bien identificado y controlado todo lo que tenga valor en su entorno para ella misma, ya sea por valor económico, o por valor funcional, o por el valor cognoscitivo, que le brinde ventaja a esa organización sobre las demás en el mercado. Por lo que es y debe ser de gran interés que es lo que se va a proteger y cuanto se piensa invertir para protegerlo. Valorar la información ha sido siempre difícil, y también hacer estos costos justificables. Establecer el valor de los datos es algo relativo, ya que la información es un recurso que no es valorado adecuadamente por ser intangible, totalmente opuesto a los equipos, la documentación o las aplicaciones. Además sumarle a esto el hecho de que las medidas de seguridad no influyen en la productividad en los procesos de las organizaciones por lo que estas son reacias a dedicar recursos a esta tarea.

Para comprenderlo de una forma gráfica, las empresas se enfrentan siempre a riesgos presentes en su entorno y las mismas tienen implementado ciertos niveles de seguridad, dos aspectos que son inversamente proporcionales, a mayores niveles de seguridad los riesgos disminuyen ya que las amenazas pierden fuerza ante la vista de la organización y por lo tanto las posibilidades de que ocurra o un ataque o una catástrofe se reducen y el riesgo que representan es mínimo o aceptable, aunque nunca desaparecen.

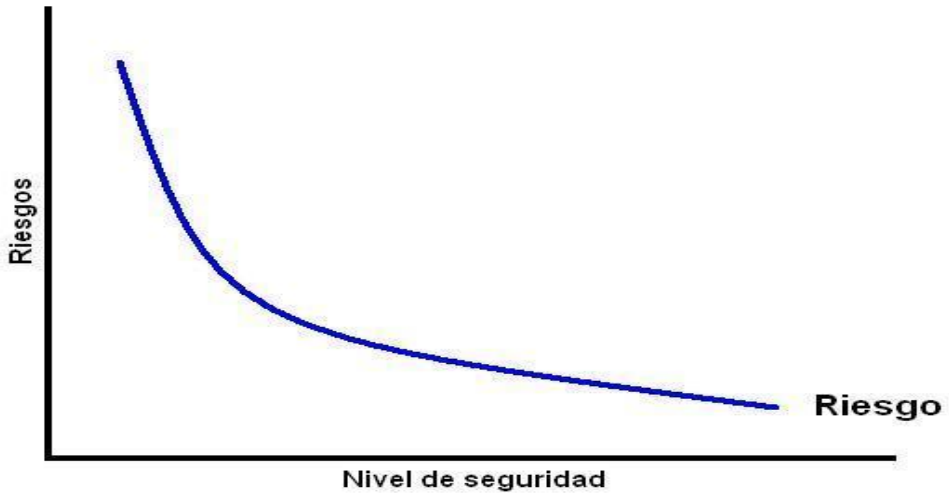


Figura 4. Gráfica Riesgos – Nivel de seguridad.

Todo lo contrario en el caso de las inversiones y el nivel de seguridad que se implemente, ya que son proporcionales directamente. Muchos autores plantean que es técnicamente imposible y financieramente incosteable lograr un sistema informático del todo seguro, pero las buenas prácticas y medidas de seguridad que se puedan tomar de acuerdo con las inversiones que haga la organización en este sentido reducen en gran medida los riesgos, y los daños que puedan ocasionar los intrusos o accidentes.

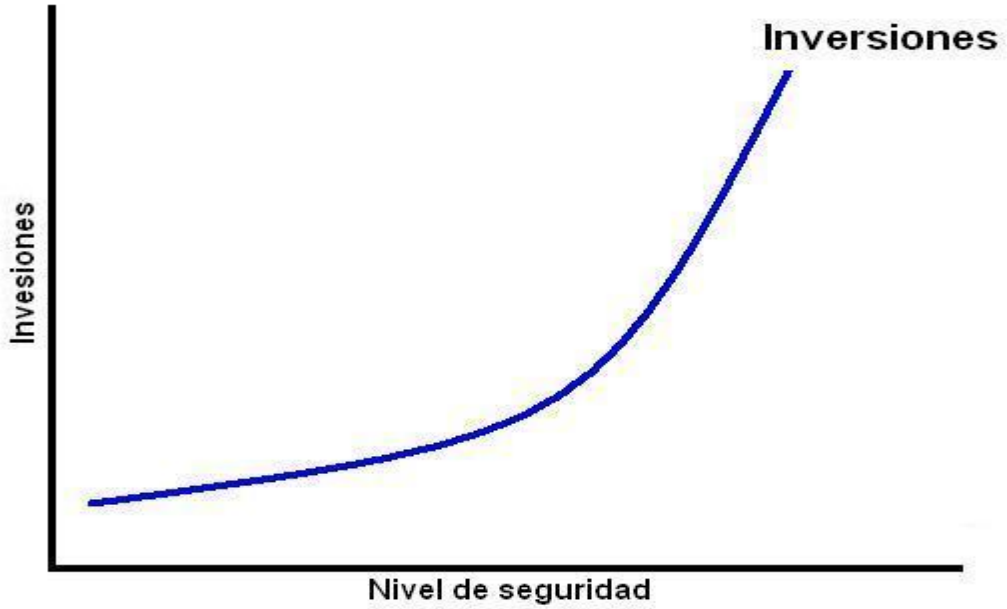


Figura 5. Gráfica Inversiones – Nivel de seguridad.

Por lo que se hace extremadamente costoso intentar implementar un nivel de seguridad cercano al ideal, pero lograremos niveles de seguridad débiles si no se invierte lo suficiente como para asegurar los activos e información de la empresa, y es aquí donde radica uno de los grandes problemas de la seguridad informática al que se enfrentan los encargados de este aspecto en una organización. Por lo que será responsabilidad y la tarea de estos encontrar el punto donde se compensan los niveles de seguridad, los riesgos y las inversiones al mismo tiempo, o sea encontrar el punto de balance o compromiso inversiones - riesgos.

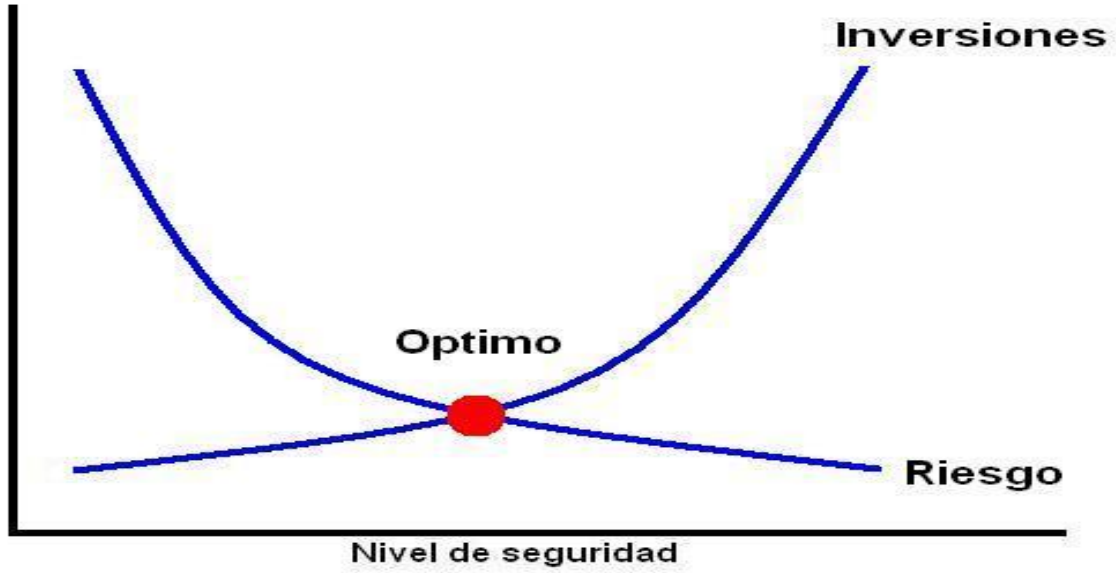


Figura 6. Punto de equilibrio Inversiones, Riesgo, Nivel de seguridad.

De esto se deriva, la necesidad de hacer un estudio sobre de que o quien se tiene que proteger los activos, que amenazas están presentes , cuales son las vulnerabilidades, los riesgos y su impacto en la organización en caso de la ocurrencia de alguno o varios.

1.3.2.3 El proceso de Gestión de Riesgos

Establecer el contexto: definir criterios sobre los cuales se efectuará la evaluación, implica tanto la definición del contexto socio-político-económico donde se desempeña la organización, como la definición de políticas y objetivos de la gestión.

Identificación: análisis, evaluación, tratamiento y monitoreo (el proceso de gestión de riesgos en sí).

Comunicar y consultar: enfocado a la necesidad de que se integre la totalidad de la organización en este proceso.

Una vez establecido el contexto se procede a:

- Identificar sistemáticamente todos los riesgos que enfrenta la organización en su conjunto
- Analizar los riesgos previamente identificados, en forma cualitativa o cuantitativa
- Evaluar los riesgos, en función de los resultados del análisis y de los criterios establecidos por la organización.
- Tratar los riesgos, de acuerdo a los resultados anteriores, se puede decidir si se lo evita, si se modifican las probabilidades o las consecuencias, si se lo transfiere, o si se lo retiene.
- Monitorear los resultados, retroalimentación, puesto que el sistema de gestión de riesgos es dinámico, se debe adaptar a los cambios de la organización y del contexto en el que opera.

De forma similar en la WhyFloos conference, Buenos Aires 2007, en un trabajo presentado por Leonardo Rosso con titulo: Eje Seguridad Informática Proyecto SOMAP.org, platea que el proceso de Gestión de Riesgos comprende los siguientes aspectos:

- ✓ Identificación y Clasificación de los Activos.
- ✓ Análisis de Amenazas y Vulnerabilidades.
- ✓ Cuantificación de la exposición y el impacto.
- ✓ Elaboración del Plan de Contramedidas.
- ✓ Evaluación del Riesgo Residual.
- ✓ Retroalimentación.

Por ser objetivo de este trabajo la obtención de un plan de seguridad informática y al enfoque más práctico de los aspectos anteriores se organizara la gestión de riesgo según estos últimos con los ajustes siguientes:

- ✓ Identificación y Clasificación de los Activos.
- ✓ Identificación de Riesgos.
- ✓ Estimación de los Riesgos.
- ✓ Plan de Contramedidas.
- ✓ Retroalimentación.

1.3.2.4 Identificación y clasificación de activos

Este proceso se realiza a partir del inventario de las organizaciones, pero más específicamente en relación a la seguridad informática se consideran los activos tangibles representados por los equipos, soportes y otros componentes de soporte y protección de la información, se realiza inventario también a la información tanto en formato digital como impreso por ser considerada la misma como un activo no tangible, el cual tiene un significativo valor para las organizaciones.

El primer paso para la realización de esta tarea es la identificación de los activos que la organización desee proteger, debido a que participa en el proceso de desarrollo de las actividades de la misma, en funciones como el procesamiento, la transmisión y almacenamiento de la información. Un segundo paso seria la clasificación de los mismos según diferentes criterios entre los que se pueden mencionar: información de contienen, actividad en la que intervienen, por ejemplo: procesamiento, transmisión o almacenamiento, naturaleza del activo, por ejemplo: hardware, software, equipamiento de redes, documentación, soporte, etc.

1.3.2.5 Identificación de riesgos

La identificación de los riesgos es crítica primero para un correcto análisis en este proceso y segundo no identificarlos pueden significar una amenaza para el éxito o cumplimiento de los propósitos de las organizaciones. Por lo que la identificación de los riesgos implica examinar todas las fuentes de riesgo y las perspectivas de todos los entes participantes ya sean internos o externos. Otro factor importante es la calidad de la información y el comprender cómo y dónde estos riesgos han tenido o pueden tener su efecto. Resulta de gran importancia que el personal a cargo esta actividad tenga, o haya obtenido en etapas previas, un amplio conocimiento de las políticas, los planes, los procesos y operaciones, que están bajo revisión. En los temas que existen un alto grado de complejidad generalmente no existen muchas personas que entiendan todos sus elementos, en este caso puede ser mejor trabajar en equipos.

Posibles fuentes de riesgo:

- Las relaciones comerciales.
- Deficiencia en actividades administrativas o controles internos.

- El alto grado tecnológico.
- Complejidad en la valoración de las mercancías involucradas.
- La complejidad de las operaciones.

Posibles áreas del impacto del riesgo:

La evaluación del riesgo puede concentrarse en uno o más áreas probables de impacto relevantes para las organizaciones en las que se pueden mencionar:

- Personal.
- Activos informáticos (hardware, software e información).
- Comunicaciones.
- Operaciones.

Métodos de Identificación de Riesgos.

Existe una gran variedad de métodos para identificar los riesgos involucrados en el contexto de una organización:

- Diagramas de flujo, técnicas de análisis de sistemas.
- Discusiones de grupo o entrevistas.
- Experiencia personal del funcionario.
- Las inspecciones físicas y auditorías anteriores.
- Brainstorming.
- Encuestas y cuestionarios.
- Técnica Delphi.
- Estudio de la experiencia extranjera o nacional.
- Los juicios, los consensos especulativos, conjeturas, intuiciones.

1.3.2.6 Identificación de Amenazas

Una vez identificados los riesgos, los recursos a proteger, se procede a la identificación de las amenazas. Como ya se mencionó existe una relación directa entre amenaza y riesgo a tal punto que si uno no existe la otra tampoco, por lo que la identificación de las amenazas, una vez que son revelados los riesgos o viceversa deberá ser una tarea más sencilla. Estas suelen ser divididas de acuerdo a su ámbito de acción:

- Desastre del entorno (Seguridad Física).
- Amenazas del sistema (Seguridad Lógica).
- Amenazas en la red (Comunicaciones).
- Amenazas de personas (atacantes internos o externos).

En las organizaciones se debería disponer de una lista de amenazas (constantemente actualizadas) para ayudar al personal encargado de la seguridad informática de las mismas en la identificación de los métodos, herramientas y técnicas de ataque que se pueden utilizar, debido el gran desarrollo de las mismas y a su rápida evolución.

1.3.2.7 Estimación de riesgo

La necesidad de medir la probabilidad de ocurrencia de sucesos dañinos para las organizaciones y los sobre los activos de las mismas en sí, de visualizar de alguna forma, ya sea cualitativamente o cuantitativamente, esas probabilidades es lo que lleva a los encargados de la seguridad en estas organizaciones a la estimación de los riesgos. La estimación constituye una base para la elaboración de las políticas y estrategias de la seguridad en la organización ya que nos ofrece información numérica o cualitativa de cuales son los activos más vulnerables, cuales son los que mayor probabilidad de daños presenta y esta información conjuntamente con la apreciación de los especialistas en el área con que cuente la organización se elaboran las medidas pertinentes para la gestión de estos riesgos.

Las técnicas o métodos de estimación más simples son los que se desarrollan en clasificaciones cualitativas, para los parámetros como: Importancia de los activos, Nivel de riesgo del activo, Integridad, Confidencialidad, Disponibilidad, Valor funcional, Valor económico. Dichas técnicas se basan por lo general en la experiencia y conocimientos técnicos de los especialistas encargados de la seguridad informáticas en las organizaciones, aunque no sean tan exactas como las estimaciones

numéricas no dejan de tener importancia ni peso a la hora de realizar un análisis de este tipo. Por otro lado las técnicas numéricas de estimación se basan en el establecimiento de escalas numéricas para los mismos parámetros y el uso de diferentes formulas para el cálculo de criterios finales por los cuales los activos son organizados por orden de vulnerabilidad ante las amenazas, mayor importancia, impacto en la organización, etc.

El método que más aparece y se hace referencia en los documentos, bibliografía y sitios web consultados es el que establece dos parámetros base para el cálculo del riesgo:

- Estimación del riesgo de pérdida del activo (**R_i**)
- Estimación de la importancia del activo (**W_i**)

Para cuantificar el riesgo de pérdida de un activo se asigna un valor numérico de 0 a 10, y de igual forma a la importancia del activo. La escala va disminuyendo de 10 a 0 en dependencia de cuan importante es el activo y cuan alto sea el riesgo de perder dicho activo. Entonces le riesgo de un activo será la multiplicación de su importancia por el riesgo de perderlo:

$WR_i = R_i * W_i$

Luego el riesgo general del activo es la sumatoria de todos sus **WR_i** dividido por la sumatoria de todas sus **W_i**, de esta forma será calculado con la siguiente ecuación:

$$WRt = \frac{(\mathrm{R1} * \mathrm{W1} + \mathrm{R2} * \mathrm{W2} \ + \cdots + \mathrm{Ri} * \mathrm{Wi})}{(\mathrm{W1} + \mathrm{W2} + \cdots + \mathrm{Wi})}$$

Se toma como ejemplo este método, y se hará uso del que se expone a continuación para el cálculo del riesgo de cada uno de los activos informáticos identificados en la empres PDVAL. Se procederá a la identificación, clasificación y ubicación de cada activo informático con que cuenta la empresa. Para la clasificación de los activos de acuerdo a la importancia que representan a la empresa se utilizara la escala siguiente:

Figura 7. Escala de importancia de activos

La equivalencia entre las categorías cualitativas y cuantitativas de la escala de la figura anterior se relaciona en la tabla que aparece debajo.

Valoración cualitativa	Equivalente cuantitativo
Muy importante	9 - 10
Importante	6 – 8
Media	3 – 5.9
Baja	1.6 – 2.9
Ninguna	0 – 1.5

Tabla #1. Relación cuantitativa - cualitativa

Se definirán también los parámetros siguientes:

Función: Importancia de la tarea que cumplen los activos informáticos.

Costo: Valor de uso de los activos informáticos.

Confidencialidad: Necesidad de proteger la información que de los activos informáticos pueda obtener.

Integridad: Necesidad de que la información no se modifique o destruya.

Disponibilidad: Que los servicios informáticos puedan ser obtenidos en todo momento de forma autorizada.

Esto no indica que se utilizaran solo estos, a criterio del analista de los riesgos, se asumirá tantos parámetros se estime conveniente utilizar para una correcta representación de los riesgos por activo y el cálculo de la importancia del mismo.

Importancia (Wi): Importancia de los activos informáticos, la cual se calculará de la siguiente forma:

$$\mathbf{Wi} = \frac{\sum \text{Parametros}}{\text{Parametros}}$$

Para el cálculo del riesgo de los activos se procederá a la identificación de las amenazas las cuales serán relacionadas en una lista y se le asignará un número consecutivo. Se obtendrá por cada activo el valor de su **Wi**, los activos serán interceptados con las amenazas identificadas, en cada intercepción será colocada la probabilidad estimada de que se concrete la amenaza sobre ese activo. Para la asignación de los valores probabilísticos se tendrá la tabla a continuación:

Nivel de Riesgo	Probabilidad
Muy alto	0.8 - 1
Alto	6 – 7.9
Medio	0.31 – 5.9
Bajo	0 – 0.3

Tabla #2. Relación cualitativa – cuantitativa Nivel de Riesgo Estimado-Valor Probabilístico.

Luego para cada activo será calculado el valor Riesgo promedio (**Ri**) que indica la probabilidad promedio de que el activo sea perjudicado por alguna de sus amenazas, dicho valor será calculado de la siguiente forma:

$$\mathbf{Ri} = \frac{\sum(\text{probabilidades de amenazas que afectan al activo})}{\text{total de amenazas que afecten al activo}}$$

Dicho valor mostrará además cuales son los activos en mayor grado propensos a ser afectados por las amenazas.

A continuación se calculará también el indicador de prioridad (**Pi**), que será igual a la multiplicación de **Ri** y **Wi**, y representara a los activos que requerirán de una mayor atención y cuidado a la hora de la definición de las medidas de seguridad. Mientras más cerca de 10 este el valor de **Pi** la prioridad de protección del activo será mayor. Y ya una vez hecho el análisis de la gestión de los riegos se tienen las bases para comenzar a elaborar las políticas de seguridad que mitigaran o administraran las amenazas con sus riesgos en el entorno de las organizaciones.

1.3.3 Políticas de seguridad

Es imposible lograr un sistema 100% seguro debido a que el costo de la seguridad total es muy alto por no decir económicamente imposible de costear. En cierto modo extremados niveles de seguridad ocasionan lentitud en los procesos e intercambio de información, tiempo extra para analizar permisos, certificados, descifrar transmisiones encriptadas, validar usuarios y claves. Este tipo de sistema de seguridad deja un espacio muy estrecho para el desarrollo de nuevos negocios para las organizaciones. Por lo que las organizaciones y entidades de todo tipo en el mundo crean documentos donde se plasman directrices, buenas prácticas, recomendaciones y estrategias orientadas y orientadoras en el uso de las tecnologías de la información, para obtener la mayor utilidad posible de las mismas, para evitar darles un uso indebido ya que las acciones irresponsables desembocan siempre en problemas que involucran la salud del sistema informático y el buen estado de la información de las organizaciones. Dentro de los planes de seguridad, las políticas de la seguridad son parte imprescindible de los mismos, las mismas son consideradas herramientas de organización y concientización para el personal de las organizaciones en las conductas que deberían seguir en sus puestos de trabajos respecto al uso de las tecnologías de la información y la información en sí, ya que es la posesión más valiosa de sus entidades.

En el mundo informático se suele restar dimensión e importancia a las políticas de la seguridad y al significado de su desarrollo, ya que las mismas no son solo un conjunto de orientaciones y

lineamientos dentro de las organizaciones, escritos en un papel y que a veces es que se aplican y ponen en funcionamiento. Las políticas de seguridad son como un producto de software que tienen un ciclo de vida, ciclo de vida que para las políticas comprende: la investigación, su creación, lograr la aceptación y aprobación por parte de la dirección de la organización, hacerla de conocimiento para toda la entidad, lograr que el personal la entienda, la acepte y la aplique en su trabajo diario, se le hace seguimiento, se actualiza y es desechada cuando esta pierde vigencia. Por lo que a la hora de confeccionarlas hay que tener estos aspectos en cuenta, para una elaboración de políticas sólidas y con un propósito bien definido.

¿Que es una política? "*Declaración general de principios que presenta la posición de la administración para un área de control definida…* " "*…son desplegadas y soportadas por estándares, mejores prácticas, procedimientos y guías…* " "*…son obligatorias y la incapacidad o imposibilidad para cumplir una política exige que se apruebe una excepción.*"[11].

Según la Guía para la elaboración de políticas de seguridad de la Universidad Nacional de Colombia, durante el desarrollo de una política esta atraviesa por 11 etapas, agrupadas en 4 fases.

1.3.3.1 Fases y etapas de una política

Las fases con sus etapas son las que se relacionan a continuación:

- Desarrollo.
  - ✓ Creación: Planificación, investigación, documentación y coordinación de la política.
  - ✓ Revisión: Evaluación independiente de la política.
  - ✓ Aprobación: aprobación de la política por la dirección.
- Implementación.
  - ✓ Comunicación: Difusión de la política entre todo el personal.
  - ✓ Cumplimiento: Implementación de la política.
  - ✓ Excepciones: Gestión de las situaciones en las que la implementación no es posible.
- Mantenimiento.
  - ✓ Concientización: Lograr que el personal la acepte y la aplique.

[11] http://www.asesoriainformatica.com/definiciones_i.htm

- ✓ Monitoreo: Seguimiento y reporte de cumplimiento de la política.
- ✓ Garantía de cumplimiento: Son las respuestas de la administración a los incumplimientos de las políticas.
- ✓ Mantenimiento: Actualización constante de la política.

- Eliminación.
  - ✓ Retiro: Prescindir de la política al estar obsoleta o no necesitarse más.

1.3.3.2 Alcance de las políticas de seguridad

Las políticas de seguridad en una organización cualquiera, están dirigidas por lo general a todo el personal de la misma, y en todas las sucursales que puedan tener estas organizaciones, pero pueden existir políticas de alcance local en un área determinada de dichas organizaciones.

1.3.3.3 Como debe ser una política de seguridad

Debe ser una forma de comunicación entre la dirección de las organizaciones y su personal, una descripción de lo que se debe proteger y el por que de ello; no es una simple descripción técnica, expresión legal que involucre sanciones a conductas indeseadas en el personal de una organización.

- Una política debe cubrir todos los aspectos relacionados con la causa que dio surgimiento a la misma.
- Debe acotarse a las necesidades y a los recursos con que se dispongan la organización.
- El tiempo en el que se aplique una política no deberá incidir en su eficacia.
- Una política deberá definir criterios y estrategias a adoptar en distintas funciones y actividades en situaciones similares para escenarios distintos.
- Claras y entendibles.
- Prácticas y realizables.
- Cooperativas y dinámicas.

1.3.4 Plan de contingencia

Los planes de contingencia son necesarios en todo sistema y no podría dejarse de lado en el tema de seguridad. Lo único que realmente permite que una empresa (o una persona) pueda reaccionar

adecuadamente a una falta en un proceso crítico es mediante la elaboración, prueba y mantenimiento de un Plan de Contingencia. El plan es precisamente lo que su nombre indica, una serie de actividades efectivas para restablecer la operatividad de la organización, en el evento de una calamidad (interna o externa). Actualmente los Planes de Contingencia formalizados y probados cobran una importancia enorme en el interior de las empresas. Estos deben obedecer a un proceso formal y debe ser el mismo personal que comience la elaboración de planes de seguridad, identificar factores críticos, establecer los equipos de trabajo y alternativas de solución de la contingencia, quien pruebe los mismos, y quien este encargado de la capacitación de las personas involucradas y su constante actualización.

La confección de planes de contingencia está comprendida en 3 etapas:

- Planificación: Actividades organizativas para el desarrollo del plan
- Elaboración: Contiene un conjunto de actividades que resultan en la confección como tal del plan.
- Aprobación y ejecución: Se expone a los niveles administrativos de la organización y en consecuencia de los resultados se pone en marcha su ejecución.

1.3.4.1 Planificación

Esta primera etapa es prioritaria ya que en la misma se desarrollan todas las consideraciones administrativas para iniciar, elaborar y poner en marcha un plan contingencia. En esta etapa deberán definirse aspectos como:

Aprobación: La elaboración del mismo debe contar desde el inicio con la autorización, apoyo y supervisión de la administración de la organización.

Organización: Deberá declararse una estructura formal, según las necesidades y el tamaño de la organización, en la que se especifiquen las responsabilidades y funciones. Dicha estructura deberá comprender preferiblemente personal de todos los niveles de la organización: personal de la administración, trabajadores y personal especializado en sistemas informáticos, soporte técnico, Redes, etc.

Alcance: Se definirán el alcance del plan y sus limitaciones, las condiciones bajo las que actuara el plan y a quien está dirigido.

Ubicación: Ubicación en la que estará el plan, el mismo deberá asegurarse que sea de conocimiento para todo el personal de la empresa y se aseguraran los respaldos necesarios para casos de pérdida o daño del mismo.

Características: En su confección el plan deberá cumplir con los aspectos: responder a las necesidades particulares de la organización, ser factible, divulgado, actualizado y probado. El mismo deberá ser presentado de forma clara de forma que facilite su evaluación y actualización, esquemático de vocabulario sencillo, adaptable y con cubiertas de material llamativo.

Capacitación: Se definirán los programas de capacitación para el personal que intervendrá en su elaboración, puesta en marcha, evaluación y corrección y actualización.

1.3.4.2 Elaboración

En esta etapa se realizan las actividades y el análisis que darán como resultado en plan de contingencia, la cual contiene de forma general las siguientes actividades:

Análisis y preparación: Se hace un análisis para de terminar la vulnerabilidad de las operaciones y se establece la estructura organizativa de los recursos necesarios, para atender y operar en la contingencia.

Atención y Recuperación: se indicaran los aspectos a seguir para la atención de las contingencias y lograr la supervivencia de las actividades de la organización.

Regreso a las condiciones normales: Los aspectos que se traten en esta sección de la fase dependerán de la magnitud de la contingencia.

Revisión y Prueba: Una vez realizado el documento de plan de contingencia, el mismo deberá ser probado con cierta frecuencia de forma modular para determinar su funcionalidad y grado de aceptación en el personal de la organización.

1.3.4.3 Aprobación y ejecución

En la misma se especifican los pasos o actividades a seguir para la presentación del plan al alto mando para su arrobación y finalmente la puesta en marcha:

Aprobación del plan: Se pondrá a consideración lo planteado en la etapa de elaboración al alto mando de la organización, por lo que los pasos a seguir serán: presentación del plan y entrega del documento para su estudio aprobación o rechazo.

Puesta en marcha: Según los resultados del análisis que la dirección de la organización realice se decidirá la puesta en marcha del mismo o la posposición del mismo hasta tanto no se corrijan los señalamientos, o sea desarrollado otro plan.

1.3.5 Auditoria informática

Primeramente se definirá el término auditoría, usado, principalmente para referirse a revisiones cuyo único fin es detectar errores, fraudes, señalar fallas y en consecuencia recomendar la "reestructuración o renovación del personal". La auditoría es un concepto más amplio, es un proceso que consiste en la determinación del grado de correspondencia del contenido informático en los sistemas de información con las evidencias que le dieron origen y en determinar si dicha información se ha generado según los principios y procedimientos establecidos. Según Fernando Catacora Carpio, Especialista en Sistemas de Información Gerencial y profesor de esta cátedra en la Universidad Católica Andrés Bello de Caracas, Venezuela, la auditoria informática "*… es aquella que tiene como objetivo principal la evaluación de los controles internos en el área de PED (Procesamiento Electrónico de Datos)*". Otro concepto seria, un "*Conjunto de procedimientos y técnicas para evaluar y controlar, total o parcialmente, un sistema o instalaciones informáticas, con el fin de proteger sus activos y recursos, verificar si sus actividades se desarrollan eficientemente…*". Por lo que una definición podría ser, revisiones planificadas o no, de un sistema informático con el objetivo de analizar y evaluar la correspondencia de la información, con la eficacia, la seguridad, la economía y la adecuación de la infraestructura informática en las organizaciones con esta información.

1.3.5.1 Alcance de la Auditoría Informática

El alcance de la Auditoría Informática será el grado de precisión con que se defina el entorno y límites en los cuales va a tener lugar la misma, complementada con los objetivos previamente señalados para realizar dicha revisión. Dicho alcance quedara plasmado de forma bien clara y concisa en el Informe final, informe en el que quedaran recogidos los temas que fueron examinados, y también aquellos que fueron omitidos.

1.3.5.2 Importancia de la Auditoría Informática

La auditoria informática es importante en las organizaciones por las siguientes razones:

- La utilización y difusión de información errónea si la calidad de los datos en los sistemas son inexactos o corruptos, pueden desencadenar una serie de problemas en cadena que pueden afectar seriamente las operaciones en las organizaciones.
- Las tecnologías de la información en cualquier ubicación se han vuelto objeto de fraudes, espionaje, delincuencia y terrorismo informático.
- Las bases de datos suelen ser objetivos de atentados y accesos de usuarios no autorizados o intrusos.
- El robo de secretos comerciales, información financiera, administrativa, la transferencia ilícita de tecnología y demás delitos informáticos.
- El Departamento de Administración de Sistemas observa un incremento desmesurado de costos, inversiones injustificadas o desviaciones presupuestarias significativas.
- Evaluación de nivel de riesgos en lo que respecta a seguridad lógica, seguridad física y confidencialidad.
- Mantener la continuidad y calidad del servicio y la elaboración y actualización de los planes de contingencia para lograr este objetivo.
- Los recursos tecnológicos de la empresa incluyendo instalaciones físicas, personal subalterno, horas de trabajo pagadas, programas, aplicaciones, servicios de correo, internet, o comunicaciones; son utilizados por el personal sin importar su nivel jerárquico, para asuntos personales, alejados totalmente de las operaciones de la empresa o de las labores para las cuales fue contratado.
- El uso inadecuado de la computadora para usos ajenos de la organización, la copia de programas para fines de comercialización sin reportar los derechos de autor y el acceso por vía telefónica a bases de datos a fin de modificar la información con propósitos fraudulentos.

1.3.5.3 Metodología de Trabajo de Auditoría Informática

El método de trabajo del auditor pasa por las siguientes etapas:

- Alcance y Objetivos de la Auditoría Informática.
- Estudio inicial del entorno auditable.
- Determinación de los recursos necesarios para realizar la auditoría.
- Elaboración del plan y de los Programas de Trabajo.
- Actividades propiamente dichas de la auditoría.
- Confección y redacción del Informe final.

1.4 Conclusión

En este sentido, es la información es el elemento principal a proteger además de los soportes de la misma en las organizaciones de cualquier tipo. Por lo que los planes de seguridad son una de las herramientas con la que se debe contar en una organización. Estos pueden estar pre-elaborados en plantillas que son adaptables pero, son únicos, y por consiguiente las políticas de seguridad estarán enfocadas a los problemas de seguridad de cada organización. Un plan de seguridad implementado y establecido para una organización resulta de un estudio de elementos y características propias de la organización que no son portables hacia otros escenarios, como las recetas médicas diagnosticadas a personas diferentes, aunque padezcan de la misma dolencia ya que el método de medicación depende de las observaciones que haga el doctor.

2 CAPITULO 2: Propuesta de Plan de Seguridad para la Empresa PDVAL

	Elaborado	Revisado	Aprobado
Nombre			
Cargo			
Firma			
Fecha			

2.1 Introducción

El Plan de Seguridad Informática refleja las políticas, estructura de gestión y el sistema de medidas que se determina en cada organización, en dependencia de las características de la misma, es la forma que tiene la dirección de una empresa de comunicar a sus trabajadores las conductas laborales que se desean imperen en la misma.

2.2 Objetivos

El Plan a continuación tiene por objetivo establecer los principios y requerimientos de seguridad de la información y activos informáticos que garanticen la confidencialidad, integridad y disponibilidad de la información que se procesa, transmite, reproduce y almacena mediante el uso de las tecnologías de información en la empresa PDVAL, además de proporcionar mecanismos y procedimientos para el aseguramiento de la misma. Será también meta de dicho plan prevenir, detectar y responder ante situaciones en las cuales se vean comprometidos en alguna forma los principios anteriormente dichos, ya sea por ataques, accidentes o negligencias del personal.

2.3 Alcance

Este plan será aplicado en todas las instalaciones de la empresa PDVAL que se encuentran por todos los estados de Venezuela, y el mismo será de obligatorio cumplimiento a todos los niveles. Por lo que es de un altísimo interés para la Gerencia de la empresa y la Administración de Seguridad Informática que el mismo sea de conocimiento por todo el personal, y que sea puesto en práctica por todos los trabajadores que realicen sus funciones mediante el uso y/o mantenimiento de las tecnologías de información de la empresa. La información que se procesa, transmite, reproduce y almacena a través de los medios informáticos de la empresa se considerará patrimonio de la empresa PDVAL, y cualquiera de las operaciones antes mencionadas deberá estar dentro de las especificaciones del siguiente Plan de Seguridad Informática. Por lo que es responsabilidad de la Administración de Seguridad Informática de la empresa y de los responsables de la seguridad a todos los niveles en la misma, el cumplimiento del plan que a continuación se expone. El presente trabajo no se referirá con la profundidad necesaria en los aspectos relativos a la seguridad del área de servidores, ya que por el momento la empresa no cuenta con una infraestructura completa de red propia, ya que dichos servidores se encuentran en un centro de datos de la empresa PDVSA, los cuales se regirán por las medidas de seguridad esta entidad.

2.4 Definiciones

PIF (Personal Informático Facultado): Personal calificado, avalado y autorizado por la Gerencia de la Empresa PDVAL o la Administración de Seguridad Informática para el cumplimiento de tareas como instalaciones y reparaciones de Sistemas Operativos y Software, además de la configuración, reparación y mantenimiento del equipamiento de la empresa cuando estos no requieran servicio especializado por la entidad contratada.

ASI (Administración de Seguridad Informática): Oficina que atenderá a nivel de la Gerencia General de la empresa los asuntos relativos a la seguridad de la información, los activos informáticos y las comunicaciones en la empresa PDVAL.

ECR (Equipo de Configuración y Reparaciones): Este es un equipo o departamento que será propuesto en este trabajo el cual estará integrado por personal que clasifique dentro de la definición de **PIF**.

DSI (Departamento de Seguridad Informática): Grupo de trabajo encargado de la dirección y gestión de la seguridad informática en la empresa PDVAL a nivel regional.

PCP (Personal de Protección y Control de Pérdidas): Personal encargado de la seguridad de las instalaciones, tanto del equipamiento de la empresa como de la mercancía que circula por estas instalaciones.

ISP (Proveedor de Servicio de INTERNET): Empresas que facilitan a otras organizaciones la conexión a INTERNET, para el caso de la empresa objeto de este plan de seguridad, PDVAL, podemos mencionar a proveedores de servicio como las empresas CANTV y MOVISTAR.

2.5 Caracterización

La empresa PDVAL cuenta con 2 servidores profesionales HP sobre el Sistema Operativo CentOS 5, en los cuales están alojados el servidor de aplicación y el servidor de bases de datos. La red de la empresa es administrada, en el área de servidores, por el personal encargado de estas funciones en la empresa PDVSA. Las estaciones de trabajo están ubicadas en las instalaciones y oficinas de la empresa PDVAL por todo el país las cuales corren sobre Sistema Operativo Windows XP, las que en su mayoría se encuentran fuera, físicamente, de la red de PDVSA, por lo que la conexión de estas estaciones con los servidores se hace mediante un cliente de conexiones SSH a través de VPN, con conexión directa a los servidores y a ningún otro servicio de la red de PDVSA, dicha red está conformada en una topología de árbol jerárquico. El nodo principal se encuentra en una de las instalaciones de la empresa PDVSA, INTVEP (Instituto Tecnológico Venezolano del Petróleo), aunque se encuentra separado lógicamente de la misma red de PDVSA, en un local acondicionado para estos fines necesarios y de accesos limitados. Dicho nodo es el único en todo el país, o sea que las conexiones de todas las instalaciones pertenecientes a la empresa PDVAL están dirigidas hacia estos servidores; a través de conexiones cableadas UTP cat5 para el caso de de las conexiones directas con la red de PDVSA, para el caso de los locales sin este tipo de conexión, se realizan mediantes módems cableados e inalámbricos. Por otra parte el equipamiento que se encuentra en las instalaciones de la empresa se ubican por lo general en oficinas cerradas de las cuales algunas carentes de climatización. El cuidado del acceso a dichas instalaciones y la protección ante pérdidas está delegada al personal de PCP que garantizan el cuidado de la institución y sus bienes fuera y durante el horario de trabajo. El control de la seguridad en la empresa PDVAL es pobre y la protección no van más allá de las

precauciones empíricas que el personal pueda tomar; pero la existencia de una estructura interna que administre la seguridad de la información y los activos informáticos de dicha empresa, está ausente, haciéndose necesario organizar de algún modo estos procesos en una organización que no es en principio compleja, pero supone un reto enorme debido al gran tamaño de la misma.

2.5.1 Aplicaciones en explotación

En los servidores se encuentran en ejecución el Sistemas Operativos CentOS 5, y el sistema SENTAI el cual corre sobre el Gestor de Base de Datos Progress e implementado sobre un lenguaje de base de datos del mismo nombre. SENTAI es un sistema de gestión empresarial y como características fundamentales que lo caracterizan podemos mencionar: que es un sistema multiusuario, permite el multiprocesamiento, es flexibilidad, parametrizable y seguro. El mismo está compuesto por **funciones** agrupadas en módulos asociados indistintamente a: **Tablas** (Registros), **Transacciones, Reportes**, **Consultas**, **Listados**, etc.

Las aplicaciones usadas en la Empresa por los trabajadores que intervienen en los procesos informáticos de la misma, para el trabajo de una oficina, se usa el paquete Microsoft Office, correo electrónico, etc., todas soportadas sobre el sistema operativos Microsoft Windows XP, adicionalmente en las estaciones de los operarios del sistema SENTAI que trabajan en las instalaciones que poseen piso de venta, cuentan con la herramienta QProg 1.70, para el trabajo con las cajas registradoras y el PC-FL1, para la configuración de las balanzas y etiquetadoras digitales.

2.6 Estructuras de Gestión de la Seguridad Informática

Ninguna actividad que se realice en una organización es realmente sólida y cumple objetivo si no hay un personal encargado de la ejecución de la misma, si no cuenta con recursos y un compromiso laboral con la misma. Por lo que para una mejor aplicación y control de la seguridad informática de la empresa PDVAL, en la propuesta de este plan, se pondrá a consideración formar e integrar a la estructura directiva-organizativa de la empresa, los siguientes componentes, Administración de Seguridad Informática (ASI) y Departamento de Seguridad Informática Compuesta (DSI), de las cuales se definirán los roles se creen necesarios para controlar y dirigir los procesos de seguridad en la empresa. Como todo plan el mismo está sujeto a cambios, reestructuraciones y el hecho de que el

mismo evoluciones y mejore, ciertamente es el deseo de la Gerencia General y del autor del presente trabajo.

2.6.1 Administración de Seguridad Informática (ASI)

La misma será la autoridad mayor en la empresa en asuntos de seguridad informática a nivel de nacional, dicha estructura no necesita de una ubicación física donde radicar, ya que no es propósito del plan la creación de nuevos locales, sino de aprovechar los recursos y personal ya existentes, por lo que los designados por la Gerencia General a desempeñar estas funciones pueden estar en sus locales habituales de trabajo y llevar estas responsabilidades desde los mismos. Las funciones que realizara esta Administración como su nombre lo indica es la de administrar, supervisar y mantener los procesos y controles de la seguridad informática de la empresa apoyándose en los DSI que se describirán más abajo.

2.6.1.1 Responsabilidades

Entre las funciones a realizar por la ASI se encuentran:

- Mantener informada a la Gerencia General del estado de seguridad de la empresa.
- Es el responsable máximo de la seguridad informática de la empresa, en todas las áreas, seguridad lógica, física, personal, procedimientos, comunicaciones, etc.
- Controlara y guiara a los DSI regionales.
- Es el encargado de la revisión y aprobación final de las modificaciones y actualizaciones que se le realicen tanto al plan de seguridad como al plan de contingencia que este incluye.
- Supervisará los simulacros de contingencia, cuando estos se ejecuten a nivel nacional.
- Es el encargado de la preparación y planificación de las capacitaciones en cuanto a seguridad del personal de la empresa
- Es el encargado de asegurar los recursos y equipamiento necesarios para llevar a cabo los procesos de seguridad en la empresa.

2.6.1.2 Los roles

Administrador de Sistema: Esta persona es el encargado de la administración del sistema SENTAI, es el responsable y único con acceso a la clave de administración (acceso como root) del sistema, solo el podrá hacer modificaciones administrativas y de configuración al sistema en caso de ser necesario. Este el encargado de realizar y supervisar las auditorias a los archivos logs del sistema cuando se realice esta actividad en la empresa o cuando ocurra un suceso que amerite la revisión de los mismos.

Administrador de Redes: Es la persona encargada supervisar la funcionalidad de la red en la empresa, responde ante la Gerencia General en los temas de conectividad, organización y mantenimientos de las redes.

Responsable de Seguridad Lógica y Comunicaciones: Esta persona responderá ante la Gerencia General por la seguridad lógica de la empresa, deberá conocer y estar al tanto sobre la adquisición y prueba de nuevos software adquiridos por la empresa, de la misma forma supervisará las comunicaciones, siempre y cuando esto no involucren a las empresas contratistas, proveedores de servicio de conexión a internet, ya que estos asuntos deberían ser tratados en un ámbito de contratos y negociaciones entre estas y la Gerencia de la empresa. Por lo que la configuración del equipamiento tanto de oficina como de actividades comerciales y comunicaciones queda bajo su supervisión.

Responsable de Seguridad Física y Operaciones: Es el encargado de la supervisión de la seguridad del equipamiento informático de la empresa, las instalaciones, responderá ante la Gerencia General por los controles de acceso a las instalaciones y al equipamiento de la misma así como la realización de los procedimientos que aseguren desde un punto de vista físico a la información y los activos informáticos de la misma.

2.6.2 Departamento de Seguridad Informática (DSI)

Este departamento deberá crearse en cada región del país en el que haya operaciones de la empresa. Por lo que su fin será realizar operaciones semejantes a la ASI pero a un nivel regional para así tener un control un poco más cerca de las actividades de la seguridad informática de la empresa. Será el encargado de llevar la gestión de la Seguridad a nivel regional, realizará las auditorias de seguridad a este nivel, registrara todas las incidencias de la seguridad en ese nivel, por lo que será misión del mismo detectar amenazas y riesgos, para crear estrategias y tomar medidas para mitigarlos, de esta forma se hará evolucionar y perfeccionar al Plan de Seguridad Informática a nivel regional para luego

realizar ajustes del mismo a nivel de ASI para asegurar de esta forma el dinamismo del mismo haciéndolo adaptable a las nuevas condiciones en la medida que pase el tiempo.

2.6.2.1 Su estructura

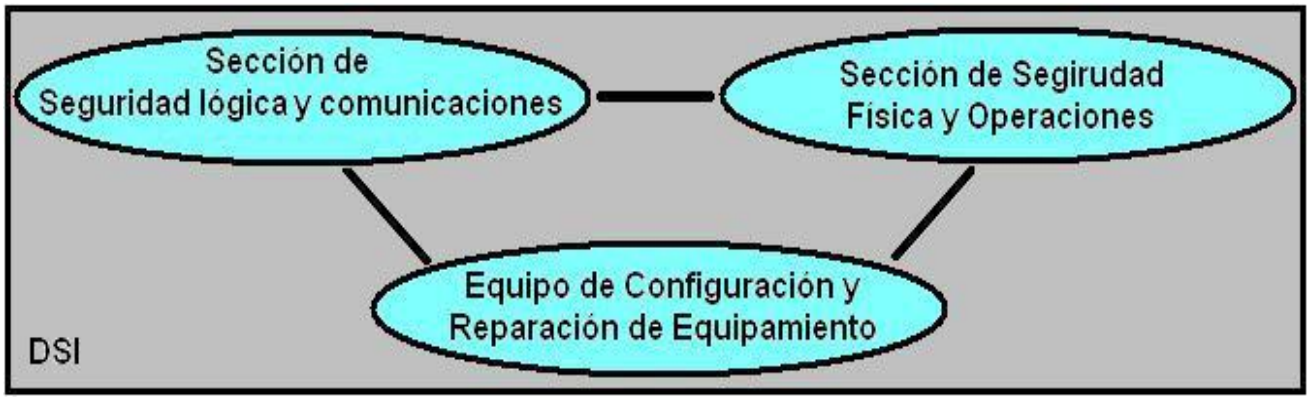


Figura 8. Estructura del Departamento de Seguridad Informática.

2.6.2.2 Las áreas

Sección de Seguridad Lógica y Comunicaciones: Su tarea será la gestión de la seguridad lógica en la región, interviene en la definición de las configuraciones del equipamiento y de la red, gestión de los permisos y accesos de los usuarios al sistema, así como la administración de los usuarios que usen el VPN como enlace con el sistema en su región y velar por que el servicio que corre en el Gateway de caja este siempre activo, así como la configuración del equipamiento de comunicaciones.

Sección de Seguridad Física y Operaciones: su tarea será la gestión de la seguridad física en la región así como velar por el correcto funcionamiento y manipulación del equipamiento. Interviene en el desensamble de equipos para recuperación y reparación, así como en la determinación que factores en las instalaciones de su región constituyen un posible amenaza para la seguridad física del equipamiento presente en estas.

Equipo de Configuración y Reparación de Equipamiento: Este equipo es el encargado de la configuración del equipamiento con vista a despliegue a las instalaciones nuevas de la región y reparación de los que presenten defectos técnicos, así como su almacenamiento y desensamble para recuperación, siempre supervisado por las secciones anteriores.

2.6.2.3 Los roles

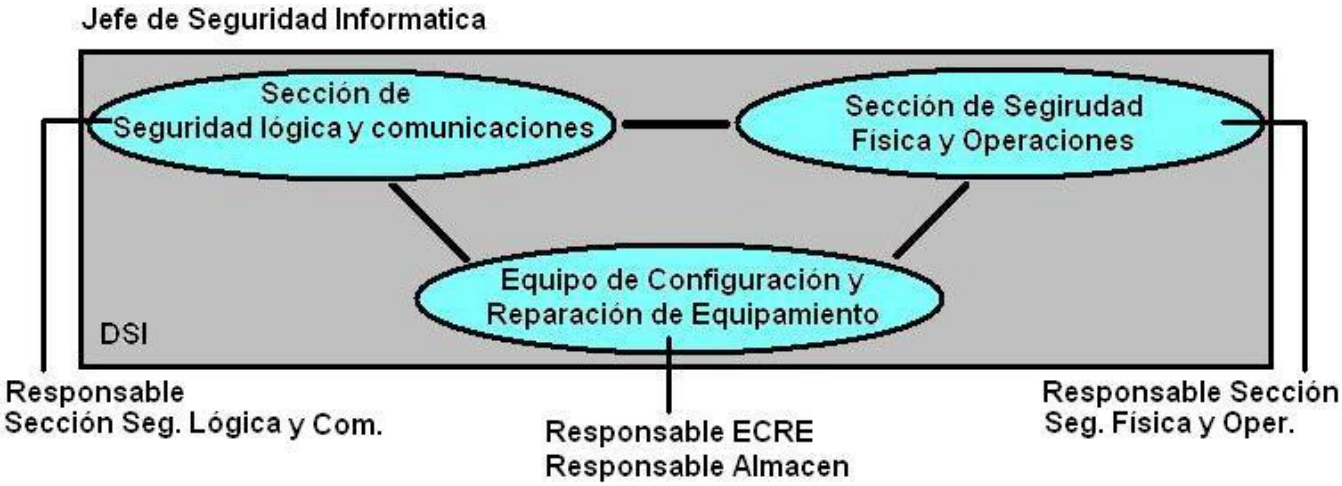


Figura 9. Responsables de áreas en el DSI

Jefe de Seguridad informática: Es el encargado de la seguridad en su región, el mismo será designado por la dirección de la región para responder ante la Gerencia General por la seguridad informática de la región. Sus responsabilidades son: llevar el control de las incidencias de la seguridad en su región, planificar y dirigir las actividades que realicen el departamento, así como mantener informada a la Gerencia General sobre todas estas actividades y además de servir como enlace entre la misma y la región respecto a comunicados y orientaciones del alto mando en lo que a seguridad respecte. Al mencionado para el logro de esta tarea se le subordinaran los siguientes cargos:

Responsable de Sección Seguridad Lógica y Comunicaciones: Es el líder de esta Sección, responde directamente al Jefe de Seguridad informática, dirige y coordina las actividades de su sección y es el receptor de los reportes de malfuncionamiento lógico de los equipos y de la red emitidos por las instalaciones de su región hacia el Departamento de Seguridad.

Responsable de Sección Seguridad Física y Operaciones: Es el líder de esta sección al igual que el anterior responde directamente al Jefe de Seguridad informática, dirige u coordina las actividades de esta sección, de igual forma es el receptor de los reportes de problemas con el cableado de datos, tomas e instalaciones eléctricas, roturas de equipamiento o malfuncionamiento de componentes mecánicos de los mismos. Su equipo se presentara también en casos de dudas o desconocimientos

de procedimientos para la operación de los equipos en las instalaciones y funcionamiento como tal del local.

Responsable de ECRE: Es el responsable del equipo, responde directamente ante el Jefe de Seguridad informática, informa sobre la completitud y estado de las tareas llevadas a cabo por el equipo, así como el estado del equipamiento que está en el almacén del departamento.

Responsable de Almacén: Este responde solamente ante el Responsable de ECRE, sobre el estado y disponibilidad del equipamiento en el almacén y lleva todo el control de los equipos que ingresan, salen y son desmontados, así como el control de los componentes que sean reusables y los que serán desechados.

2.6.3 Control de la Seguridad en las instalaciones

Se reitera que no es objetivo de el autor, que se amplíe la plantilla de los trabajares en la empresa PDVAL, así que debido a que el equipamiento en las instalaciones es realmente poco y el número de instalaciones es muy grande, colocaremos las responsabilidades de la seguridad informática sobre los usuarios de dicho equipamiento, ya que no entorpecerá para nada en su trabajo el asumir estas responsabilidades. El DSI siempre realizará la supervisión de las instalaciones por lo que si ocurre alguna incidencia que el mismo personal de la instalación no cuente con los medios para solucionarla estos intervendrán, por lo que la estructura de la gestión de la seguridad en la empresa quedara de la siguiente forma.

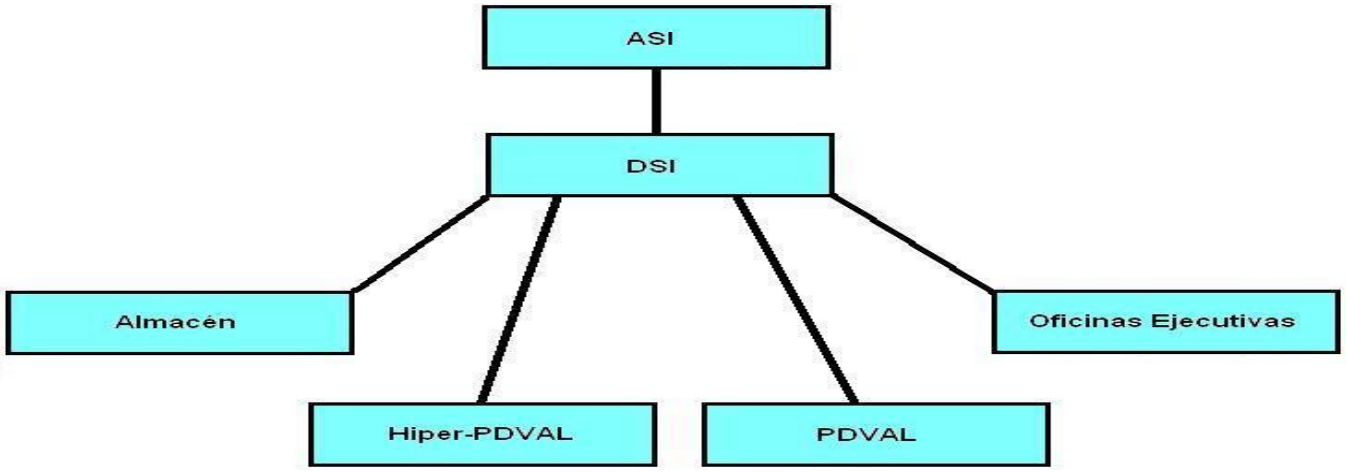


Figura 10. Jerarquía de control de la Seguridad Informática

2.6.3.1 Responsabilidades en las instalaciones

Los responsables de la seguridad en las instalaciones de la empresa son los que se muestran en la figura y se describen a continuación.

Figura 11. Responsables de la Seguridad Informática en las entidades de PDVAL.

Responsable de Seguridad Informática: Esta persona es el administrador de la instalación, el cual aparece solamente en los locales en que se señalan (Híper-PDVAL y PDVAL). Responderá ante el DSI regional por las condiciones físicas y del entorno en el cual se encuentra el equipamiento de la instalación, además de estar al tanto de que no haya ningún tipo de pérdida de información en su local, que las comunicaciones estén en funcionamiento y del estado de los equipos para este fin que estén presentes en su instalación además que la información que se almacena, genera e imprime en su local esté segura.

Operador de Sistema: Este responde ante el Responsable de Seguridad Informática, vela por el buen funcionamiento y estado de salud de la computadora en la cual trabaja, se hace cargo además de la impresora y en caso de no estar conectado directamente con la red de la Empresa, será responsabilidad suya el Modem inalámbrico, así como la información de la empresa y de su entidad en particular que se almacene en su computadora.

Supervisor de Cajas Registradoras: A su cuidado estarán las cajas registradoras en el piso de venta es el encargado de supervisar la correcta manipulación de estos equipos así como la ejecución de acciones que requieren de su nivel de autorización. Es el encargado de sacar de la caja la cinta auditora y entregársela inmediatamente al administrador (Responsable de Seguridad Informática) o al que deje en su representación, por lo general al financiero.

Jefe de Almacén: Le será entregada la custodia de las balanzas digitales y las etiquetadoras digitales, por lo que velará por su correcto uso, e informará inmediatamente al administrador (Responsable de Seguridad Informática) cualquier problema con el funcionamiento de estos equipos.

En cualquiera de los niveles y ubicación, las incidencias de la seguridad que tengan lugar serán registradas por el DSI como tal para llevar el control en este sentido y luego realizar estudios para erradicar o mitigar las consecuencias que puedan ocasionar la ocurrencia de las mismas.

2.7 Análisis de Riesgos

2.7.1 Los activos

A continuación se relacionan los activos informáticos con los que cuenta la empresa.

Descripción	Tipo	Ubicación
Servidores HP	HW	Centro de Datos (INTVEP).
Base de Datos	GD	Servidores Centro de Datos (INTVEP).
Sistema SENTAI	SW	Servidores Centro de Datos (INTVEP).
Gateway de Cajas Registradoras (computadora)	EC	Centro de Datos (INTVEP).
Impresoras Xerox Phaser 3428	HW	Oficinas de la empresa (ejecutivas, operadores de sistema).
PC	HW	Oficinas de la empresa (ejecutivas, operadores de sistema).

Herramienta de configuración de cajas registradoras QProg 1.70	SW	PCs de las oficinas de la empresa (operadores de sistema).
Cajas Registradoras Quorion QMP 3226	HW	Pisos de Venta (PDVAL, Híper-PDVAL)
Scanner fijos Metrologic 7320	HW	Pisos de Venta (PDVAL, Híper-PDVAL)
Balanzas Digitales Digit SM 300	HW	Pisos de Venta (PDVAL, Híper-PDVAL)
Etiquetadoras Digitales Digit DP 90	HW	Almacenes (PDVAL, Híper-PDVAL)
Switchs NetGear JFS-516	EC	Oficinas de la empresa (ejecutivas, operadores de sistema).
Routers CISCO 1800 series	EC	Oficinas de la empresa (ejecutivas, operadores de sistema).
Módems Inalámbricos	EC	Oficinas de la empresa (ejecutivas, operadores de sistema).

Tabla #3. Relación de activos, tipo y ubicación de los mismos en la empresa PDVAL.

Descripción: Descripción de los activos informáticos (equipo, marca, modelo).

Tipo: Tipo de activos informáticos:

GD: Sistemas de gestión de datos

HW: Hardware

SW: Software

EC: Equipos de Comunicaciones

Ubicación: Local donde se encuentran los activos informáticos.

2.7.1.1 El equipamiento

Servidores: La empresa cuenta con dos servidores profesionales Hewlett Packard (HP)

Computadoras: La empresa, en abril de 2008 firma el primer Anexo al Convenio Marco, en el cual se contempla los Servicios Profesionales para la Configuración, Instalación, Programación e Implementación de la plataforma, así como la dotación del componente tecnológico requerido para instalar el sistema informático SENTAI e implantar 2 Híper-PDVAL, 228 PDVAL, 24 Almacenes y 25 Jornadas/Operativos. De un total de 266 instalaciones (almacenes, Híper-PDVAL, PDVAL). Para los cuales la distribución de computadoras es: tres para los Híper-PDVAL, dos para los PDVAL y una computadora para los Almacenes. Por lo que la empresa al momento de este levantamiento de equipamiento contaba con 486 computadoras Lenovo, HP y COMPAQ, en este tipo de instalaciones más un total de 26 en las dos oficinas gerenciales presentes en Caracas.

Switchs NetGear JFS 516: Estos dispositivos están ubicados en los locales de ventas y almacenes, que pertenecen a la empresa, en el caso de los Almacenes que son rentados, se extiende un punto de red del cableado de la instalación para la computadora que estará en el local rentado

Routers CISCO 1800 series: Estos dispositivos se encuentran en los locales a los cuales hace falta realizar un sub-netting debido a la cantidad de equipos con interfaces de red que requieren conexión en estos locales, dígase algunos PDVAL, Híper-PDVAL y oficinas ejecutivas.

Módems: Estos son ubicados en los locales a los cuales no se puede extender la red de PDVSA y su conexión es vía telefónica a través de ISP (Internet Servicie Provider) como CANTV o MOVISTAR.

Impresoras: En todas las instalaciones hay una impresora con la cual se realizan las impresiones de los reportes que se hacen periódicamente durante el día en cada una de ellas. En el caso de los locales donde se realizan ventas nos referimos a los partes de ventas que tienen que informar a la presidencia de la empresa, además de otro tipo de documentación que se tiene que registrar de las operaciones que se realizan; en el caso de los almacenes se imprimirían las entradas y salidas de mercancías en los mismos así como los estados de inventario que el responsable del almacén tiene que tener actualizados. En las oficinas ejecutivas, por supuesto también tenemos al menos una impresora en cada una.

Cajas Registradoras: Estas se encuentra en todos los PDVAL e Híper-PDVAL, son los equipos utilizados para realizar las ventas de los productos en estos locales y son los equipos que generan gran parte de la información de la empresa y de ellas depende la actualización de la base de datos, ya

que las ventas que se realizan diariamente en todas los pisos de venta de la empresa, deben ser ingresados diariamente a la base de datos y cualquier dificultad con estos equipos conlleva a un atraso en la actualización de la base de datos, ya que el proceso seria necesario realizarlo manualmente y la Gerencia de la empresa contaría con datos inciertos si se fiara de la información contenida en la base de datos.

Balanzas y Etiquetadoras y Scanner: Estos equipos son los menos importantes de la empresa pero no dejan de jugar un papel en el desempeño de las actividades principalmente de ventas en los pisos de venta de la empresa, agilizan el tráfico de clientes y humanizan el trabajo al personal que trabaja directamente con los clientes.

2.7.2 Importancia de activos

Es de suma importancia determinar cuales son los activos importantes de la organización y cual seria el impacto que produciría si llegasen a faltar o fallar, por lo que la pregunta para clasificarlos es: ¿qué efecto tendría en la empresa si el activo faltase o fallase? Al clasificarlos podemos agrupar los activos y así hacer la tarea del análisis menos complicada, para concentrar los esfuerzos en los activos de mayor importancia en la empresa y luego los de menor jerarquía. Para ellos usaremos la escala que aparece en la Fig. #4 y la Tabla #1.

A continuación se muestran la importancia de los activos relacionados según los criterios de valoración que aparecen en esa columna, para determinar la importancia total de cada uno de ellos.

Activo (descripción)	**Parámetros**					**Importancia (Wi)**
	Función	**Costo**	**Confidencialidad**	**Integridad**	**Disponibilidad**	
Servidores HP	10	8	10	10	10	9.6
Base de Datos	10	10	10	10	10	10
Sistema SENTAI	10	8	10	10	10	9.6
Gateway de Cajas Registradoras	8	6	10	10	10	8.8
Impresoras Xerox Phaser 3428	5	6	5	-	7	4.6

PC	9	6	8	8	10	8.2
Herramienta de configuración de cajas registradoras QProg 1.70	7	-	5	10	7	5.8
Cajas Registradoras Quorion QMP 3226	9	5	7	10	10	8.2
Scanner fijo Metrologic 7320	5	3	-	5	-	4.3
Balanzas Digitales (Digit SM 300)	4	5	4	10	4	5.4
Etiquetadoras Digitales (Digit DP 90)	4	5	4	10	4	5.4
Switchs NetGear JFS-516	8	6	10	10	10	8.8
Routers CISCO 1800 series	9	6	10	10	10	9
Módems Inalámbricos	8	6	10	10	10	8.8

Tabla #4. Importancia de activos informáticos de la empresa PDVAL.

Por lo que en orden de importancia tendremos la siguiente relación

Activo (descripción)	**Importancia (Wi)**
Base de Datos	10
Servidores HP	9.6
Sistema SENTAI	9.6
Routers CISCO 1800 series	9
Gateway de Cajas Registradoras	8.8
Switchs NetGear JFS-516	8.8
Módems Inalámbricos	8.8
PC	8.2
Cajas Registradoras Quorion QMP 3226	8.2
Herramienta de configuración de cajas registradoras QProg 1.70	5.8
Balanzas Digitales (Digit SM 300)	5.4

Etiquetadoras Digitales (Digit DP 90)	5.4
Impresoras Xerox Phaser 3428	4.6
Scanner fijo Metrologic 7320	4.3

Tabla #5. Activos por orden de importancia para la empresa PDVAL

2.7.3 Amenazas

Las amenazas a las que se expone la empresa PDVAL son las que se enumeran a continuación de acuerdo a las observaciones de los especialistas y técnicos de la corporación CIMEX que prestaron servicios con el autor del presente trabajo durante la misión:

1) Fallo de las comunicaciones.
2) Falla del fluido eléctrico.
3) Fallas en el Hardware.
4) Capacitación del personal.
5) Mala manipulación del sistema que se utilizan en la empresa.
6) Mala manipulación de la información.
7) Filtración de información clasificada entre el personal no autorizado.
8) Malas configuraciones del equipamiento informático.
9) Mala manipulación de equipos digitales en los puntos de ventas de la empresa.
10) Virus informáticos.
11) Robos de tecnologías informáticas.
12) Acceso pirata en la red por personal no autorizado.
13) Incendios.

2.7.3.1 Consecuencias

Es preciso especificar cuales son las consecuencias que acarrean las amenazas identificadas anteriormente, ya que esto servirá para dar una visión del impacto que pueden tener en la empresa además de servir de base para la elaboración del plan de contingencia adjunto a las medidas para la seguridad informática propuestas en este plan. En la tabla a continuación se especifican las consecuencias de por amenazas.

Amenaza	Consecuencias
Fallo en las comunicaciones.	1. Impide la recuperación de la información en las cajas registradoras. 2. Impide la actualización del fichero PLU en las cajas. 3. Impide los procesos de facturación de las ventas. 4. Impide los procesos de generación y recepción de transferencias, ordenes de venta, pagos, etc. 5. Retrasos en la documentación de las entidades. 6. Desactualización de la base datos del sistema.
Falla del fluido eléctrico.	1. Cese de las operaciones comerciales en las instalaciones. 2. Fallos de configuración en los equipos digitales. 3. Corrupción o pérdida de la información en los equipos digitales.
Fallas en el Hardware.	1. Incapacitación de los equipos 2. Corrupción o pérdida de la información.
Capacitación del personal.	1. Lentitud en las operaciones de la empresa. 2. Errores en operaciones del sistema. 3. Corrupción o pérdida de información.
Mala manipulación del sistema que se utilizan en la empresa.	1. Corrupción o pérdida de información. 2. Desactualización de la base de datos del sistema. 3. Retrasos en los procesos de la empresa
Mala manipulación de la información.	1. Pérdida de documentos. 2. Mal estado de la información. 3. Retrasos en los procesos de la empresa. 4. Desactualización de la base de datos del sistema.
Filtración de información clasificada entre el personal no autorizado.	1. Accesos no permitidos en el sistema. 2. Atentados directos al sistema y la información. 3. Robo, pérdida o corrupción de información. 4. Robo de mercancía.
Malas configuraciones del equipamiento informático.	1. Corrupción de la información. 2. Accesos no permitidos. 3. Robo de información.

Mala manipulación de equipos digitales en los puntos de ventas de la empresa.	1. Corrupción o pérdida de información. 2. Incapacitación de los equipos. 3. Retrasos en los procesos de la empresa.
Virus informáticos.	1. Corrupción o pérdida de información. 2. Incapacitación de los equipos. 3. Retrasos en los procesos de la empresa.
Robos de tecnologías informáticas.	1. Pérdida de información. 2. Incapacitación de los equipos. 3. Retrasos en los procesos de la empresa. 4. Reposición de los equipos.
Acceso pirata en la red por personal no autorizado.	1. Robo o destrucción de información. 2. Incapacitación de la empresa. 3. Retrasos en los procesos de la empresa.
Incendios	1. Pérdida de información. 2. Incapacitación de los equipos. 3. Retrasos en los procesos de la empresa. 4. Reposición de los equipos.

Tabla #6. Consecuencias de las amenazas en caso de que ocurriesen.

2.7.4 Estimación de Riesgos

De acuerdo con las amenazas identificadas se cuantifica el riesgo de que cada una de ellas se materialice sobre cada uno de los activos informáticos, lo que en este caso se realizara de forma numérica, se asignarán valores entre 0 y 1 (0 sí la probabilidad de materialización de la amenaza es nula y 1 sí es máxima), según la clasificación como se observa en la Tabla #2.

Se utilizarán las amenazas anteriores y la Tabla #2, se obtiene la siguiente, en la que se relacionan los activos, las probabilidades de ocurrencias de cada amenaza para cada uno de ellos, los riesgos promedio, importancia y la prioridad relativa a cada uno de los activos.

Activo	Amenazas													Ri	Wi	Pi
	1	2	3	4	5	6	7	8	9	10	11	12	13			
Base de Datos	0.8			0.5	0.3	0.3	0.1					0.1		0.35	10	3.5
Servidores HP	0.8											0.1		0.45	9.6	4.32
Sistema SENTAI	0.8			0.5	0.3	0.3	0.2					0.1		0.36	9.6	3.46
Routers CISCO 1800 series	0.7	0.3									0.1		0.1	0.3	9	2.7
Gateway de Cajas Registradoras	0.4			0.3			0.3			0.1				0.27	8.8	2.38
Switchs NetGear JFS-516	0.1	0.3									0.1		0.1	0.15	8.8	1.32
Módems Inalámbricos	0.8	0.3	0.1	0.1							0.3		0.1	0.28	8.8	2.46
PC	0.3	0.2		0.3			0.4			0.9	0.1		0.1	0.33	8.2	2.71
Cajas Registradoras Quorion QMP 3226	0.5	0.6	0.3	0.4		0.4		0.4	0.4				0.1	0.39	8.2	3.20
Herramienta de configuración de cajas registradoras QProg 1.70				0.3		0.2								0.25	5.8	1.45
Balanzas Digitales (Digit SM 300)		0.6	0.2	0.3				0.3	0.3		0.1		0.1	0.27	5.4	1.46
Etiquetadoras Digitales (Digit DP 90)		0.6	0.1	0.3				0.4	0.3		0.1		0.1	0.27	5.4	1.46
Impresoras Xerox Phaser 3428		0.3						0.1			0.2		0.1	0.18	4.6	0.83

Scanner fijo Metrologic 7320	0.6	0.2	0.2	0.1	0.1	0.1	0.22	4.3	0.95

Tabla #7. Cálculo de prioridad de protección de los activos informáticos.

Riesgo promedio (Ri): Valoración del riesgo sobre cada bien informático es el promedio de las columnas Probabilidad de ocurrencia de las Amenazas.

Importancia (Wi): Importancia de los activos informáticos.

Prioridad (Ri * Wi): Prioridad de atención en relación a la seguridad sobre cada activo informático, es la multiplicación de los valores Riesgo promedio e Importancia.

Luego de los cálculos el peso en cuanto a riesgos de los activos de la empresa queda de la siguiente manera

Activo (descripción)	**Prioridad**
Servidores HP	4.32
Base de Datos	3.5
Sistema SENTAI	3.46
Cajas Registradoras Quorion QMP 3226	3.20
PC	2.71
Routers CISCO 1800 series	2.7
Módems Inalámbricos	2.46
Gateway de Cajas Registradoras	2.38
Balanzas Digitales (Digit SM 300)	1.46
Etiquetadoras Digitales (Digit DP 90)	1.46
Herramienta de configuración de cajas registradoras QProg 1.70	1.45
Switchs NetGear JFS-516	1.32
Scanner fijo Metrologic 7320	0.95
Impresoras Xerox Phaser 3428	0.83

Tabla #8. Relación de activos por Prioridad

Y en base a esta tabla se tomarán las medidas necesarias para la seguridad de los activos de la empresa según la prioridad de la tabla.

2.8 Sistema de Medidas para la Seguridad Informática

Debido a la necesidad de organizar las actividades relacionadas con el empleo de la informática, el uso y explotación de los equipos y programas, en interés del aseguramiento de las actividades de la empresa PDVAL, se incluye las siguientes medidas para garantizar la seguridad y confiabilidad de la información que se elabora, procesa y transmite mediante los equipos informáticos de dicha empresa. Omitir o violar dichas medidas propuestas en el Plan, deberán ser considerados como indisciplinas laborales, es responsabilidad por orden y según la cadena de mando, de la Gerencia General conjuntamente con los Departamentos de Seguridad Informática Regionales, las direcciones en todos los niveles y trabajadores, principalmente que trabajan con el equipamiento informático de la empresa, velar por el cumplimiento de las mismas, y aplicar las medidas disciplinarias pertinentes en consecuencia con la gravedad de la misma, según dicte el reglamento disciplinario de la organización.

2.8.1 Medidas administrativas y organizativas

- La Gerencia General conjuntamente con la ASI deberá garantizar los recursos necesarios para hacer cumplir el Plan de Medidas de Seguridad Informática en la empresa.
- Todo el personal que haga uso de las tecnologías de información tiene que conocer el Plan de Seguridad Informática de la empresa.
- Todo el personal que trabaje con las tecnologías de la información debe conocer los procedimientos:
  - ✓ Para evitar la pérdida de información.
  - ✓ Para evitar la pérdida de equipamiento.
  - ✓ Del Plan de Seguridad Informática.

2.8.2 Medidas respecto a la información

- El personal autorizado para procesar la información clasificada y sensible, deberá cumplir a cabalidad las medidas para la protección de la información, los equipos y locales de la empresa.
- Cada soporte magnético, óptico o plano con información clasificada tendrá una etiqueta de control debidamente identificada (Anexo 2).
- El soporte magnético, óptico o plano con información clasificada contara con un registro de uso de soportes de información (Registro 2), en el cual se reflejaran todas las actividades que se realicen con estos soportes.
- En los locales que permanezcan los soportes con información clasificada y sensible se cumplirán además de las exigencias técnicas requeridas, las medidas de protección física que se establezcan.
- Los soportes con información clasificada o sensible se almacenaran en archivos o estantes bajo llave y sello.

2.8.2.1 Soportes de información

- La Gerencia General conjuntamente con la ASI debe controlar la asignación de soportes para back-up o salvas para los servidores y las computadoras en las oficinas de las instalaciones de la empresa.
- Cada entidad resguardará los soportes de información de interés particular.
- Se guardan bajo llave los soportes que se utilicen para resguardar la información. Estas llaves estarán a la custodia del responsable de la Seguridad en la entidad.
- En los DSI regionales deberá existir un Banco de Software, del cual se hará responsable el jefe del DSI.
- En los Bancos de Software estarán los soportes de los Sistemas Operativos, Drivers y aplicaciones o programas utilizados en las entidades así como los que contienen documentación del sistema y manuales del equipamiento desarrollados en la empresa.
- El control de todos estos soportes, será realizado mediante el Registro 6 (Control de Soportes).

Los soportes de información que serán empleados en la empresa para el procesamiento y almacenamiento de información son:

- Discos duros de los servidores
- Discos duros de las estaciones de trabajo.
- Discos de salva de la información
- Soportes ópticos (discos).
- Papel.

2.8.2.1.1 Conservación

- Los soportes del Banco de Software se conservarán en un archivo cerrado con llave y sellado que reúna las condiciones requeridas en cuanto a temperatura, humedad relativa y resistencia al fuego.
- Sólo está autorizado para manipular los soportes del Banco de Software el Jefe del DSI regional.
- Los soportes del Banco de Software no serán objeto de préstamos.
- Antes de entregarlos y/o recibirlos, el responsable de los mismos comprobará la correspondencia de su contenido contra la lista de nombres que aparece en la etiqueta y en caso de ser soportes magnéticos se escanearan en busca de virus informáticos.
- La entrega-recepción de soportes de la información será controlada a través del Registro 7.
- La información de uso diario en las diferentes entidades deberá estar protegida en un local o en archivo metálico, bajo llave y en lugares protegidos.
- La información clasificada deberá duplicarse y estar bajo la custodia del Responsable de la Seguridad Informática de la instalación.

2.8.2.1.2 Destrucción

- Los DSI serán los únicos encargados y autorizados de realizar esta tarea.
- La destrucción se llevara a cabo mediante herramientas informáticas para este fin o mediante el formateo a nivel físico de las unidades en caso de haberse encontrado en soportes magnéticos, o se destruirán los documentos y soportes ópticos mediante trituración e incineración.
- Al culminar la ejecución de esta tarea el Jefe de DSI regional emitirá un Acta de Destrucción de Información (Anexo3), la cual será archivada y notificada a la ASI.

Traslado

- Para el traslado de soportes que contengan información fuera de las entidades u oficinas de la empresa se deberán tomar las siguientes medidas:

- El Responsable de la Seguridad Informática de la instalación y los DSI son los únicos facultados para autorizar el traslado de información fuera estas.
- La información será trasladada en un sobre cerrado y sellado.
- La persona que lo traslada es responsable de su custodia y entrega en el lugar indicado.

2.8.2.2 Clasificación de la Información

La información que se manipula en la empresa son por lo general documentos contables y de circulación de mercancía, obligaciones de pago y demás por parte del área comercial, en cuanto al área técnica se maneja los ficheros de configuración de de los diferentes equipos que se despliegan a los locales para el uso del sistema. Por lo que se propondrán las siguientes categorías para la información:

Clasificada: Esta categoría de información le será impuesta a aquellos documentos e información a la cual solo podrán tener acceso estrictamente los directivos de la empresa y aquellos trabajadores cuyas funciones dependan o se basen en la manipulación de la misma. Representaran aquella información mediante la cual la empresa puede quedar expuesta a un ataque o que su pérdida o corrupción puede afectar gravemente en las operaciones de la misma.

Sensible: La categoría identificara a la información que solo deberá conocer el personal o grupo de trabajo que realice sus funciones con este tipo de información, aunque no represente un problema si es conocida por otro personal interno, deberá cumplirse el principio inicial. Representara aquella información que en manos mal intencionadas, las consecuencias no irían más allá de especulaciones, difamaciones sobre la empresa, pero la misma no desea que se conozca de todas formas.

Ordinaria: Será la categoría otorgada a la información que no representa amenazas para la empresa en caso de caer en manos ajenas a la empresa, puede ser conocida por todo el personal de empresa, pero no de dominio publico.

Publica: Será la información de la empresa de dominio para el público; dicha información será liberada por la misma empresa con un fin informativo para la población en general.

Una vez presentadas las categorías de información, los documentos e información tanto digital como en formato duro se clasificaran de la siguiente forma:

Clasificada:

- ✓ Claves de acceso a los servidores.
- ✓ Claves de acceso al sistema como root (Administrador).
- ✓ Back-up de la base de datos.
- ✓ Ficheros logs del sistema.
- ✓ Listado de cuentas bancarias.
- ✓ Ficheros de configuración de los equipos del piso de ventas, (cajas registradoras, balanzas digitales, etiquetadoras digitales, etc.).
- ✓ Ficheros de configuración del soporte de comunicaciones, (Switchs, Routers).

Sensible:

- ✓ Cinta auditora de la caja registradora.
- ✓ Reportes de ventas diarias.
- ✓ Facturas.

Ordinaria:

- ✓ Transferencias.
- ✓ Ordenes de venta y compra.

Publica:

- ✓ Listado oficial de precios.

2.8.3 Medidas respecto al personal

- Se seleccionará y autorizará por el Departamento de Recursos Humanos conjuntamente con el Departamento de Seguridad los niveles de acceso del personal.
- El personal de mantenimiento y limpieza podrá permanecer en los locales en los que se encuentre equipamiento informático siempre que estén acompañados por el personal que sea responsable del local o supervisor de esta actividad.

- Los nombres y respectivos cargos de las personas autorizadas a permanecer en los locales donde se tenga equipamiento de soporte de comunicaciones o almacenamiento de información serán colocados en la puerta de acceso al mismo.
- Al igual que la información sobre estos locales se llevara un control mediante un registro de acceso (Registro 4).
- Los trabajadores no operarán los recursos informáticos sin estar previamente adiestrados y autorizados por el DSI Regional, al que estén subordinados.
- Los trabajadores que realizan funciones con el equipamiento informático de la empresa, al causar baja de la misma, la dirección de la entidad a la que pertenece informará al DSI Regional, el cual asegurará que en el futuro no puedan tener acceso a los activos informáticos de la red, por lo que será eliminarse la cuenta de usuario de dicho trabajador.
- Todo usuario del sistema informático es absoluto responsable de la veracidad y exactitud de la información que introduce en el sistema, almacene, transporte y entrega.

2.8.4 Medidas de seguridad Física

2.8.4.1 Áreas a proteger

Debido a la gran magnitud de la empresa y a la variedad de las instalaciones con que cuenta la misma, en las cuales se ha desplegado y se desplegara el sistema, la heterogeneidad en los locales es elevada por lo que se describirá las áreas que deberán existir en todas las instalaciones sin importar lo diferentes que sean. A continuación se relacionan y a su vez la importancia que estas representan para la empresa:

- Cuarto de Servidores: imprescindible.
- Oficinas ejecutivas de la empresa: muy importante.
- Oficinas de operadores de sistema: importante.
- Almacenes: importante.
- Pisos de venta: publica.

2.8.4.2 Barreras Físicas

- Las PCs, impresoras, y el equipamiento de soporte de comunicaciones de las instalaciones deberán estar en locales seguros, separados por paredes, de materiales no combustibles, del resto de los locales de la instalación.
- Los locales deberán contar con techos, sin forma de acceso aéreo, y preferentemente sin ventanas en caso de tenerlas, es recomendable enrejar dichas ventanas.
- Las puertas de acceso a los locales deberán tener cerradura, de forma tal sean accesibles sin llave solo desde adentro.
- En horarios no laborales estos locales deberán permanecer cerrados y las llaves no deberán salir de la instalación; se le entregará en custodia al personal encargado de la seguridad y protección de la instalación.
- De la misma forma los cableados deberán estar protegidos por algún tipo de cobertura, tubos metálicos, canaletas plásticas, o por el interior de la pared, nunca deberán estar al descubierto.

2.8.4.3 Mecanismos de protección Física aplicados

Los equipos de mayor confidencialidad e importancia para la empresa son los servidores de aplicación y bases de datos sobre los cuales corre la aplicación para la administración de la misma, al encontrarse estos servidores dentro de instalaciones de la empresa PDVSA, cuentan con la seguridad implementada por esta en las instalaciones de INTVEP en Caracas. Por lo que la seguridad física de estos está asegurada, ya que los mecanismos de ingreso y restricción de acceso a las áreas de dicha instalación son buenos, pues cuentan con un sistema de control de acceso por tarjetas de proximidad, así como protocolos de acceso estrictos. De esta forma los servidores gozan de las medidas de seguridad del centro de datos de la instalación mencionada.

- En las oficinas de las instalaciones la seguridad del equipamiento queda delegada a los usuarios de dichos equipos.
- Deberá existir al menos un extintor de gas carbónico en cada oficina de las instalaciones de la empresa.
- La toma eléctrica y los puntos de red deberán estar en buen estado y bien instalados, siempre elevados del suelo.
- Los equipos deberán estar lejos de áreas húmedas.

- Se deberá tener en los locales UPS, para garantizar la continuidad de los procesos en la empresa durante un intervalo de tiempo en el cual falle el sistema eléctrico.
- Se deberán habilitar estabilizadores de voltaje, ya que los equipos con que se trabaja son altamente sensibles, para la protección contra fluctuaciones de voltaje.
- Los circuitos eléctricos del equipamiento deberán estar separados en fases distintas a la de los aires acondicionados, motores eléctricos, etc.
- Se deberán habilitar archivos metálicos con cerradura para la protección de la documentación e información, y los soportes magnéticos u ópticos de la misma.
- Los locales deberán estar climatizados, así poder extender el tiempo de vida útil de los equipos.
- Los equipos de soporte de las comunicaciones de los locales serán colocados en racks para su protección y una mejor organización en la administración de la red LAN de cada local.
- El DSI sellará todo el equipamiento de la empresa para limitar el acceso a los componentes internos de los equipos.
- El DSI es el único con potestad de remover el sello, ya que es el organismo rector de la Seguridad Informática de la Región además de ser el encargado de la configuración y reparación de estos equipos.
- Las PC y servidores deben protegerse contra posibles hurtos, o sustracción de sus componentes, así como el robo de discos duros y los archivos de las entidades, por lo que se establecerá el acceso limitado y controlado a cada local donde se encuentre este tipo de activos.
- Deberá garantizarse que las tecnologías informáticas sean utilizadas solo por el personal autorizado.
- Al conectar o desconectar equipos a la red eléctrica, los mismos deberán estar apagados.
- Los circuitos de alimentación eléctrica para las tecnologías informáticas deben ser independientes de la red eléctrica común del local, y separado de aquellos que alimentan equipos de fuerza o altos consumos.
- El equipamiento informático fundamental para la continuidad de las operaciones en la empresa, deberá estar conectado a fuentes de respaldo de energía con estabilizadores de voltaje.
- Las cintas auditoras de las cajas registradoras serán tratadas como información sensible para la empresa, las cuales en cada instalación de la misma deberán almacenarse, debidamente identificadas y separadas por bolsas en las que estarán las cintas de un día.

- El traslado de equipos fuera de las instalaciones tendrán siempre un responsable, quien deberá portar un documento del DSI que autorice los movimientos de estos medios y quedara reflejado en el Registro de Incidencias de la Seguridad Informática (Registro 1) de las instalaciones por las que transite.
- Se prohibirá el consumo de alimentos y bebidas en los locales en los cuales se encuentre equipamiento informático, para asegurar la integridad de los mismos.
- La entrada o estancia de personas en áreas reservadas será controlada, bajo la previa autorización del Jefe de dicha área. En el caso del personal de servicio, mantenimiento de equipos u otro que eventualmente precise permanecer en el área estará siempre acompañado de las personas responsables u otras designadas por estas.
- Las claves de acceso a los servidores de la empresa como root (Administrador) serán custodiadas, en un sobre cerrado independiente y bajo llave, por el Jefe de Seguridad Informática, de la Gerencia General.

2.8.4.4 Control de Acceso a las Tecnologías de la información

- Al cuarto de servidores sólo tendrán acceso el personal de la ASI por parte de la Gerencia General.
- Los trabajadores que necesiten para su trabajo el uso de las tecnologías informáticas y de comunicaciones, sólo podrán hacerlo en los medios que tienen asignados.
- Para que un trabajador utilice otra máquina de su oficina u otra oficina deberá ser autorizado por el Responsable de la Seguridad Informática de la instalación correspondiente y debe estar presente algún trabajador de esta área durante el período de tiempo que se trabaje.
- Los DSI tendrán acceso total al equipamiento de la empresa que requiera sus servicios, siempre en compañía de una de las personas responsabilizadas con dicho equipamiento, en caso de necesitar el equipo ser trasladado al taller del DSI, este asume la responsabilidad del mismo
- El equipamiento que vaya a ser retirado de la instalación por el DSI se le deberá realizar una salva de la información más importante y se borrara la memoria de dicho equipo antes de la salida.
- Deberá asegurarse de que las puertas permanezcan cerradas para evitar el acceso a personal no autorizado.

- El control de ingreso y salida del personal visitante o ajeno a la empresa a las instalaciones es responsabilidad del personal PCP con que cuente la instalación. Incluyendo a las oficinas de los operadores de sistema y demás locales.
- El movimiento del equipamiento informático deberá ser plasmado en el Registro de Entrega-Recepción (Registro 7) en el que quedará constancia del traslado.
- El jefe del ECRE deberá llenar el Registro de mantenimientos a equipos (Registro 5), donde hará constar las tareas realizadas sobre los distintos equipos por el ECRE de la región.

2.8.4.5 Sistema de control de Acceso

Los relacionados a continuación tendrán acceso absoluto a todos los locales de la empresa:

- ✓ La ASI por parte de la Gerencia General para controlar y verificar el cumplimiento de las medidas orientadas.
- ✓ Los Jefes de DSI para controlar y verificar el cumplimiento de las orientaciones pero a nivel regional
- ✓ El Administrador de la Red para los trabajos relacionados con la misma.
- ✓ Miembros del equipo de auditorias de la empresa cuando estén en función de esta tarea.

- Cada persona que acceda a los locales contemplados por este Plan, que sus funciones no estén ligadas a esa área, si hace uso del equipamiento, esto será anotado en el Registro de Acceso correspondiente al área (Registro 4) por el responsable de la misma.
- El Registro 4 será revisado mensualmente por el Responsable de Seguridad Informática de la instalación.
- El acceso a las instalaciones de la empresa es controlado por el personal de PCP
- El acceso a los locales donde se encuentran activos informáticos por personal visitante o ajeno a la empresa es concedido por el Responsable de Seguridad Informática de la instalación al igual que para el personal de servicio y mantenimiento.
- El solapín de cada trabajador establece el nivel de acceso en las oficinas en o áreas de las instalaciones de la empresa.
- Para el caso de los visitantes a las oficinas de las instalaciones, la recepción llama por teléfono a la persona que será visitada y ésta autoriza la entrada, por lo que se habilita un pase temporal (solapín).

- El visitante deberá esperar a que la secretaria confirme la autorización de acceso.
- El acceso de los trabajadores será a los locales correspondientes a su área de trabajo y también a las áreas relacionadas con su trabajo con la debida autorización.
- A las oficinas Administrativas de las instalaciones sólo tiene acceso autorizado los Responsables de la Seguridad o Administrador de la instalación, el personal operador de sistema, el personal financiero, de Recursos Humanos, el DSI y la ASI.
- El personal de limpieza y mantenimiento podrán acceder a todos los locales siempre acompañados por el personal que trabajan en esas oficinas o por un encargado a esta tarea, por lo que realizaran sus funciones siempre acompañados por alguien.
- El personal que se encuentre en prestación de servicios tendrá una autorización por escrito mientras permanezca en las instalaciones.
- La entrada, salida y traslado de equipamiento serán autorizados por el Responsable de Seguridad, por el Administrador o Director de la instalación, el equipamiento antes de dejar la instalación deberá pasar por la recepción con el correspondiente documento, se puede mantener el que está vigente pero se anexa en el plan el siguiente modelo (Anexo 4); constatar en el Registro de entrada-salida y movimiento de equipamiento (Registro 3).
- La permanencia fuera del horario laboral es autorizada por el Responsable de la Seguridad Informática de la instalación.

2.8.5 Medidas de seguridad Lógica

- La información será priorizada por orden de importancia: la integridad (prevenir modificaciones no autorizada), la disponibilidad (prevenir retención no autorizada) y la confidencialidad (prevenir divulgación no autorizada).
- El equipamiento y los soportes que sean utilizados en las jornadas, no podrán contener información sensible ni que comprometa de alguna manera la gestión de la empresa.
- Deberá realizarse un chequeo previo y posterior de todos los medios y los soportes utilizados en las jornadas.
- Todo nuevo software que llegue a empresa, antes de poner en explotación, será sometido a un proceso de certificación, que garantice, dentro de límites razonables, que satisface los requerimientos en cuanto a seguridad y prestaciones que debe ofrecer.

- Se controlará de forma sistemática todo el software que se encuentra autorizado para su explotación en la empresa.
- La custodia, revisión, actualización y prueba de los ficheros de configuración estándar para cada modelo de equipamiento quedaran bajo la responsabilidad del ECR, en PCs aisladas de la red o en soportes como: discos o dispositivos externos de almacenamiento masivo.
- Se deshabilitaran la reproducción automática y el booteo desde los puertos USB y las unidades de disco CD/DVD.
- La reparación o mantenimiento de los equipos, dígase: Servidores, Routers, Switchs, Módems, PCs, Cajas Registradoras, Balanzas Digitales, Etiquetadoras Digitales, etc.; solo se ejecutara una vez borrada la memoria de dichos equipos.
- Solo se utilizara la herramienta QProg 1.70 para la actualización del fichero PLU (listado de productos y precios) en caso de no haber conexión con el sistema.
- Durante la venta no se ejecutaran actualizaciones de precios ni ajustes de configuración a ningún equipo en las áreas de venta.

2.8.5.1 Protección de acceso a las Tecnologías de Información

- En los DSI el ECRE implementará la contraseña del Set-up en todas aquellas PC que el modelo lo permita, por lo que es de gran importancia y preferentemente aquellas que procesan información.
- Se le configuraran contraseñas también a las balanzas digitales y a las etiquetadoras digitales, y para el caso de las cajas registradoras el DSI no entregará la llave PWO (programador) de dichas cajas para proteger la configuración de estos equipos.

2.8.5.2 Identificación y Autenticación de Usuarios

Para el inicio de sesiones en la PC

A los operadores de sistema, se les habilitara una cuenta de usuario estándar para poder acceder a la PC, con una clave que le será entregada y solo será conocimiento de los operadores del sistema que trabajen en dicha maquina y del Responsable de la Seguridad informática de la instalación.

Para el acceso al sistema:

Los operadores deberán introducir su identificador y su clave que solo será revelada al usuario por parte del DSI para ingresar al sistema. La clave para ingresar al sistema será responsabilidad exclusiva del usuario.

Para la conexión con la red PDVSA:

Esta variante es para el caso de los operadores de sistema que su maquina no está conectada directamente con la red de PDVSA, y tienen que hacer un enlace mediante un VPN a través de INTERNET.

Como en las otras especificaciones, el usuario deberá introducir un identificador y una clave para acceder a la red de PDVSA a través del VPN y luego iniciar su sesión en el sistema de la forma anteriormente explicada, dicha clave también le será revelada solamente al usuario.

2.8.5.3 Claves

- Las claves de acceso deben combinar números, letras, mayúsculas y minúsculas, caracteres especiales y tener una longitud de al menos 10 caracteres.
- Las claves serán cambiadas en cada cambio de usuario (vacaciones, relevos de cargo, bajas, etc.), cuando sean conocidas por dos o más personas y al vencerse el tiempo establecido para su renovación. (recomendación, cada 3 meces).
- En sentido general para todas las claves que se usen en la empresa se deberán seguir las siguientes indicaciones:
  - ✓ Deberá estar compuesta por al menos 10 caracteres.
  - ✓ Al menos 2 caracteres en mayúscula.
  - ✓ Al menos 2 caracteres en minúscula.
  - ✓ Al menos 2 números.
  - ✓ Al menos 2 caracteres especiales (#, $, +, etc.).
  - ✓ Al cambiarlas no deberá ser igual a las anteriores 5 claves.
  - ✓ No deberán contener caracteres sustitutos como ($ como s ó S, @ como a ó A).
  - ✓ Se cambiaran las claves cada 3 meces, deberá configurarse un e-mail para recordar esto a los trabajadores.
  - ✓ Es responsabilidad de cada trabajador proteger su o sus claves.

2.8.5.4 Traza de auditoria sobre acciones que amenazan la seguridad

Se realizaran revisiones cada mes de las trazas del sistema, para detectar intentos de accesos no autorizados y verificar la integridad de los procesos y datos del servidor. Dichas revisiones estarán bajo la supervisión del Administrador del sistema el cual creara una comisión con este fin.

2.8.5.5 Protección contra programas dañinos

Se contará con los productos antivirus certificados en los diferentes locales donde existan computadoras, y se mantendrán los mismos debidamente actualizados. En este caso las diferentes distribuciones del antivirus Kaspersky, es una buena opción para contrarrestar la aparición de virus en la red, en los dispositivos de almacenamiento masivo portables y en soportes ópticos que puedan infestar las maquinas de la empresa.

Queda prohibido el uso de soportes magnéticos que no pertenezcan a la empresa, excepto los autorizados por los Jefes de DSI, y los responsables de la seguridad informática en las entidades y las oficinas.

El DSI es el responsabilizado de someter los sistemas, programas de aplicaciones, documentos y archivos en general, adquiridos a través de INTERNET o por otra vía, a un “proceso de cuarentena” contra programas dañinos.

No se adquirirán copias de software de procedencia desconocida.

En caso de detectar un virus desconocido el Responsable de Seguridad Informática en el local que se detecte informara inmediatamente al DSI regional, y este será el encargado de aislarlo. Si resulta imposible la descontaminación manual se procederá a retirar la computadora para descontaminarla en los talleres del DSI.

Se prohíbe terminantemente el intercambio de códigos de virus entre personal o grupo de trabajo en la empresa. Es responsabilidad del DSI y únicamente de este.

2.8.5.6 Control de acceso

En los servidores se mantendrán actualizadas las cuentas de usuario, se eliminarán aquellas que corresponden a usuarios que causan baja de la empresa, que se encuentren de vacaciones, o sustituciones en el cargo, se crearán nuevas cuentas a los que se incorporen por primera vez.

2.8.6 Medidas de Seguridad de Operaciones

2.8.6.1 Salvas

- Se realizara diariamente de forma automática a las 2:30 am una salva (Back-up) en ambos servidores de la información de la misma.
- El Back-up realizado por lo servidores deberá ser copiado en un soporte magnético o hacia otra PC aislada de la red.
- Deberá tenerse todas las instalaciones de los sistemas, Drivers y herramientas usadas por la empresa en soportes ópticos o magnéticos, asegurados en locales acondicionados para este fin.
- Todos los operadores de sistema deberán realizar salvas de la información que se genera diariamente en sus localidades u oficinas.
- El sistema en uso por la empresa debe tener salvas externas de todos los ficheros que lo integran dígase: ejecutables, índices, tablas, etc.; en soportes debidamente identificados y aislados de la red de la empresa.
- Deberá efectuarse sistemáticamente salvas de la información de los servidores y del software de las aplicaciones que se utilizan en la entidad.
- La frecuencia con que se realizaran estas salvas dependerá de la actualización de la información y las aplicaciones.
- Los dispositivos de almacenamiento que contengan las salvas del sistema deberán estar guardadas bajo llave y en un lugar donde los riesgos de incendio, inundación, campos magnéticos fuertes, radiación, altas temperaturas, etc., sean mínimos.

2.8.6.2 Mantenimiento y reparación de medios técnicos

El personal encargado de estas actividades será el ECRE.

La reparación y mantenimiento, del equipamiento se efectuara cada 6 meses, justo después de las auditorias.

El desarrollo y la instalación de nuevos sistemas informáticos son responsabilidad del DSI así como el mantenimiento de los que se encuentran en explotación.

2.8.6.3 Control del uso, traslado y entrada de tecnologías de información

- El equipamiento de la empresa que vaya a ser trasladado hacia las instalaciones que pertenecen a la misma deberá realizarse en transportes aptos para esta función y preferentemente con techo.
- Deberá existir libro de registro donde se controla el movimiento de todos los medios informáticos.
- El equipamiento reemplazado o retirado de las instalaciones debido a limitaciones o defectos técnicos, será llevado ante el ECRE para su recuperación, de no ser posible, será utilizado como pieza de repuestos, por lo que dejará de existir como equipo y será clasificado por piezas reutilizables. Las cuales estarán también bajo el mismo control que los equipos.
- Todo el equipamiento que se va a trasladar hacia las instalaciones a las cuales se desplegara el sistema, deberán ser configurados y revisados por el ECRE, antes de salir hacia sus designaciones.

2.8.6.4 Controles Periódicos

Para la realización de estos controles los que inspeccionan reflejaran todo el proceso en el Registro 8.

Los controles periódicos se llevaran a cabo trimestralmente por equipos conformadas o designadas por el DSI conjuntamente con la Gerencia General de la empresa, para realizar estas revisiones.

Los equipos mencionados anteriormente tienen la misión de realizar un control de las medidas y procedimientos de seguridad informática llevados a cabo en las instalaciones de la empresa. Por lo que las actividades a realizar son:

- ✓ Inspeccionar el local donde se encuentra el equipamiento.
- ✓ El equipamiento.
- ✓ La información.
- ✓ Estado de las comunicaciones.

- ✓ Los procedimientos internos de la instalación.

2.8.6.5 Medidas educativas o de concientización

Se informará y pondrá al alcance de todos los usuarios de la empresa el plan de seguridad informática de la misma.

Deberá de asegurarse de que todos conozcan y dominen las exigencias de dicho plan.

Al trabajador que realice sus funciones en un ordenador se le instruirá en buenas prácticas de uso y cuidado de la computadora, mediante medios digitales e impresos.

Se impartirán encuentros, cursos y conferencias cada año para que los usuarios conozcan los cambios y actualizaciones que se realicen al plan de seguridad de la empresa.

Se realizan propagandas impresas cada mes, sobre aspectos del sistema y de las políticas de seguridad informática, que deben ser de dominio general en todos los empleados de la empresa, para minimizar los niveles de ocurrencia de violaciones de la seguridad informática.

Una vez por semana el Responsable de la Seguridad Informática de la instalación tendrá una charla con todos los trabajadores de la misma sobre un tema del plan y la seguridad en general.

2.8.6.6 Capacitaciones

La Gerencia General conjuntamente con la ASI y los DSI deberán planificar, cursos de capacitación en los siguientes aspectos, Configuración, mantenimiento y reparación del equipamiento así como seminarios de seguridad informática y temas relacionados, siempre se agrupará al personal según el área en que trabajan y a la estrategia que tenga la Gerencia en este sentido:

- ✓ Equipamiento informático de la empresa
- ✓ Seguridad informática

- Se deberá capacitar en el correcto uso de las tecnologías de la información que se trasladen hacia sus entidades y en el correcto uso del sistema informático SENTAI.
- Las capacitaciones deberán ser en forma de cursos formales que tributen al expediente laboral del trabajador, no enseñanzas sobre la marcha.
- Se debe asegurar que el personal que trabajará en las diferentes instalaciones de la empresa cuenta con la capacitación necesaria para realizar sus funciones, antes de comenzar a desempeñarlas.

- Deberá ser interés de la Gerencia General proporcionar los recursos necesarios para un correcto desempeño de estas actividades.

2.8.6.7 Sanciones

- Se aplicaran las medidas correspondientes de conformidad con lo establecido en el Reglamento Interno de Disciplina Laboral.
- Son conductas sujetas a medidas disciplinarias al usar los servicios de la red las siguientes acciones:
  - ✓ Los intentos no autorizados de conexión.
  - ✓ Envío de mensajes amenazadores, racistas o relacionados con sexo.
  - ✓ Extracción o envío de información o de productos que usa la empresa a personal no autorizado.
  - ✓ Envío de cartas de cadena a través del correo electrónico o hacer uso inapropiado de los recursos.
  - ✓ Utilización del tiempo y los recursos de la entidad para beneficio personal.
  - ✓ Robo o copia de ficheros electrónicos sin permiso.
  - ✓ Utilización de los servicios con fines ajenos al objetivo de trabajo para el cual fue autorizado.
  - ✓ Negarse a cooperar con una investigación de seguridad.

2.8.7 Medidas generales

- El personal designado a ocupar responsabilidades en el DSI debe ser altamente confiable.
- Las PC de cada entidad deberán estar libres de información que no corresponda a la función para las que fueron destinadas, dígase archivos de tipo: documentos personales, foto, video, juego, música, etc.).
- Se prohibirá el uso de los medios de computación de la empresa para el uso y procesamiento de información ajena a los intereses de misma.
- En caso de pérdida de manuales o dudas con las operaciones que puedan poner en peligro la confidencialidad, integridad o disponibilidad de la información, se debe informar

inmediatamente al responsable de Seguridad Informática en la entidad y este a su vez al DSI regional al que este subordinado.

- Para utilizar soportes de propiedad personal o de otra Entidad, será necesario contar con la autorización del Responsable de la Seguridad Informática de la instalación u oficina, el cual será el responsable de que a su salida no contengan información sensible para la empresa.
- Durante la venta se desconectaran las cajas registradoras y solo serán conectadas en los siguientes casos: actualización de PLU, obtención de partes y reportes y configuraciones autorizadas.
- Se establece con carácter obligatorio el uso de los registros de Incidencias para los locales de la empresa donde se utilicen las tecnologías informáticas, y en los mismos se anotarán todos aquellos eventos de interés especial dentro de la seguridad informática.

2.9 Registros

2.9.1.1 Registro No. 1 (Registro de Incidencias para la Seguridad Informática)

En este registro (Anexo 5) se reflejaran todas las incidencias o sucesos relacionados con la seguridad de la empresa, el mismo deberá existir en todas las instalaciones de la empresa, en el mismo quedaran reflejados los siguientes datos:

- ✓ Numero consecutivo
- ✓ Fecha del hecho
- ✓ Hora del hecho
- ✓ Hecho detectado
- ✓ Numero de solapín de quien detecto la misma
- ✓ Nombre y apellidos de quien detecto la misma
- ✓ Área de la seguridad que se vio involucrada

2.9.1.2 Registro No. 2 (Registro de Uso de Soportes de Información)

Este registro (Anexo 6) es que refleja la utilización de los soportes de información, en el se reflejaran todos los movimientos del mismo con los datos que se presentan a continuación:

- ✓ Numero consecutivo
- ✓ Solapín del solicitante.
- ✓ Nombre y apellidos.
- ✓ Código del soporte.
- ✓ Actividad a realizar.
- ✓ Fecha y hora, de inicio y fin del trabajo con el soporte.

2.9.1.3 Registro No. 3 (Registro de Entrada-Salida y Movimiento de Equipamiento)

Este registro (Anexo 7), es de suma importancia que en el queden reflejados todos los movimientos de equipamiento que tienen lugar en una instalación cualquiera de la empresa:

- ✓ Fecha y hora
- ✓ Datos del equipamiento: Marca, Modelo, Serial
- ✓ Procedencia
- ✓ Destino
- ✓ Motivo del movimiento
- ✓ Nombre de quien autoriza
- ✓ Firma de quien autoriza
- ✓ Observaciones

2.9.1.4 Registro No. 4 (Registro de Acceso)

(Anexo 8). Será de principalmente usado por el personal de PCP, para el control del personal que entra y sale de las instalaciones de la empresa:

- ✓ Local o área
- ✓ Solapín de quien accede (número de cédula caso de ser visitante)
- ✓ Nombre y apellidos de quien accede
- ✓ Solapín de quien autoriza
- ✓ Nombre y apellidos de quien autoriza
- ✓ Firma de quien autoriza
- ✓ Motivos del acceso

- ✓ Fecha
- ✓ Hora de ingreso
- ✓ Hora de salida

2.9.1.5 Registro No. 5 (Registro de Mantenimiento de Equipamiento)

Este registro (Anexo 9) será llenado por el personal de ECRE del DSI, cada vez que realicen cualquier actividad de configuración, mantenimiento o reparación del equipamiento informático de su región:

- ✓ Fecha
- ✓ Equipo: Marca, Modelo, Serial
- ✓ Solapín
- ✓ Nombre del técnico
- ✓ Trabajos realizados
- ✓ Observaciones

2.9.1.6 Registro No. 6 (Registro de Control de Soportes)

En este registro (Anexo 10) se llevara el inventario de los soportes que entran y son dados de baja en los locales habilitados para estas funciones:

- ✓ Código o serial del soporte
- ✓ Contenido fundamental del soporte
- ✓ Clasificación de la información
- ✓ Fecha y hora de entrada
- ✓ Fecha y hora de baja
- ✓ Observaciones

2.9.1.7 Registro No. 7 (Registro de Entrega-Recepción de Soportes)

Este registro (Anexo 11) es que refleja la utilización de los soportes de información, no será usado en forma de libro, ya que cuando se use un soporte, este quedara en el estante en lugar del soporte y será archivado luego del proceso de devolución:

- ✓ Numero consecutivo
- ✓ Numero del soporte
- ✓ Entrega:
  - Nombre, solapín y firma de quien entrega
  - Nombre, solapín y firma de quién recibe
  - Fecha y hora de entrega
  - Objetivo de utilización
- ✓ Recepción:
  - Nombre, solapín y firma de quien devuelve
  - Nombre, solapín y firma de quién recibe
  - Resultado de la comprobación de la lista de nombres
  - Resultado del escaneo de virus
  - Fecha y hora de recepción
- ✓ Observaciones

2.9.1.8 Registro No. 8 (Registro de Inspecciones)

Será el documento que el grupo de inspección llevara para el control de las instalaciones (Anexo 12):

- ✓ Fecha de la Inspección.
- ✓ Instalación objeto de inspección
- ✓ Participantes
- ✓ Situaciones Detectadas
- ✓ Plan de Medidas
- ✓ Responsables del Cumplimiento
- ✓ Evaluación de la inspección
- ✓ Observaciones

2.10 Auditoria

- Deberá realizarse auditorias interna a las instalaciones semestralmente y una general anualmente al sistema de seguridad informática que se ha implementado en esos periodos.

- A cargo de las auditorias internas cada 6 meces estarán los DSI.
- A cargo de las auditorias anuales estará la ASI conjuntamente con la Gerencia General y apoyada por los DSI regionales.
- Se revisaran los resultados de las auditorias anteriores para lograr eliminar los señalamientos hechos al sistema, y así actualizar y perfeccionar el plan de seguridad de la empresa.
- Supervisar el proceso de captación, generación y salva de la información en las diferentes áreas de la instalación según el equipamiento que se utilice en cada una de ellas.
- Supervisar el manejo, estado técnico y acondicionamiento del equipamiento.
- Recoger en los registros de auditorias los eventos siguientes de relevancia para la Seguridad Informática
    - ✓ Revisiones de accesos, según puesto de trabajo y usuarios.
    - ✓ Hora, día, mes y año del acceso.
    - ✓ Movimiento de equipamiento en el que ha estado involucrada la instalación.
    - ✓ Almacenamiento y seguridad de la documentación e información con que se trabaja en la instalación.
    - ✓ Estado de las comunicaciones.
    - ✓ Estado y protección del equipamiento.
    - ✓ Revisión a los procedimientos internos.
    - ✓ Aspectos de interés.

2.11 Plan de Contingencia

2.11.1 Aspectos Generales

El Plan de Contingencia tiene en cuenta las amenazas y vulnerabilidades a las que están expuestas las tecnologías informáticas y la información en la empresa PDVAL. Por lo que se prestara más atención en este plan a la sostenibilidad de las comunicaciones, salvas de la información en los servidores y a la documentación.

Debido a la estructura propuesta para la implantación y control del plan de seguridad informático, la activación y actualización del plan de contingencia seguirá la misma estrategia del plan de seguridad informática. Por lo que los DSI conjuntamente con el administrador de la red y el administrador del sistema por parte de la Gerencia General serán los principales actores en las activaciones del plan de

contingencias así como su actualización y ensayos en las diferentes regiones. Pero estos se apoyaran principalmente en los responsables de la seguridad informática en las entidades y las oficinas de la empresa.

Con el objetivo de comprobar que tan rápido la empresa puede recuperarse y que el personal de la misma está preparado para la puesta en marcha del plan de contingencia según la situación dada, se realizaran simulacros de catástrofes. Dichos simulacros tanto a nivel regional como nacional serán dirigidos, supervisados y evaluados por la Gerencia General conjuntamente con los DSI regionales. Cada vez que se culminen estas pruebas se deberán hacer correcciones al plan de contingencia en consecuencia con las dificultades presentadas en los procedimientos de recuperación y puesta en marcha de la empresa por parte del personal de la misma.

2.11.2 Vulnerabilidades

Se Utilizará la tabla de consecuencias por amenazas identificadas en la gestión de los riesgos, los sucesos que pondrán en marcha del Plan de Contingencia son:

- ✓ Fallo en las comunicaciones.
- ✓ Falla del fluido eléctrico.
- ✓ Fallas en el Hardware.
- ✓ Errores en operaciones del sistema.
- ✓ Robo de información.
- ✓ Filtración de información clasificada entre el personal no autorizado.
- ✓ Corrupción o pérdida de información de las cajas registradoras u otro equipo digital.
- ✓ Incapacitación de los equipos.
- ✓ Accesos no permitidos.
- ✓ Virus informáticos.
- ✓ Acceso pirata en la red por personal no autorizado.
- ✓ Incendios

2.11.3 Matriz de acciones por contingencia

A continuación se detallan las acciones a tomar en cada caso, por etapas, quienes son los responsable de atender la contingencia.

Contingencia: Fallo en las comunicaciones.

Etapas	**Quien Detecta**	**Responsables**	
		Responsable de Seguridad Informática	**DSI**
Información	Informa al Responsable de Seguridad Informática		

Neutralización	Inspecciona la configuración de conexión. Inspección de las conexiones física.	Ingresa al local de equipos de comunicaciones, inspecciona conexiones físicas y funcionamiento de los equipos.	De no resolverse la situación informar al DSI regional el cual deberá: Inspeccionar la conectividad de la red hacia la instalación. Inspeccionar la configuración de los equipos de comunicaciones. Y si el problema persiste informar a la ASI para que tramite la situación con los ISP contratados.
Recuperación	Realiza las anotaciones en el Registro 1		Realiza las anotaciones en el Registro 5

Contingencia: Falla del fluido eléctrico.

Etapas	**Quien Detecta**	**Responsables**		
		Operador de sistema	**Responsable de Seguridad Informática**	**DSI**
Información	Informa al Responsable de Seguridad Informática			
Neutralización		**Pisos de Venta**		En caso de ser

		Realiza la salva de la información que están en las cajas y la imprime, luego apaga los equipos de la oficina	Orienta que el personal que trabaja en el piso de venta y el personal de PCP desalojen de clientes el mismo y a la supervisora de cajas que retire las cintas auditoras de las mismas y apague los equipos. Todas las mercancías que estaban en movimiento vuelven a su lugar de origen. Coordinar todas las acciones.	una avería del circuito eléctrico de la instalación y estar dentro de sus posibilidades solucionarlo este procederá. De lo contrario informara a la ASI y se procederá a la contratación de personal especializado.
		Oficinas y Almacenes		
		Guarda todos los cambios de las operaciones que estaban en ejecución y apagar los equipos	Coordinar todas las acciones.	
Recuperación	Realiza las anotaciones en el Registro 1		Informará la finalización de las actividades y la puesta en marcha de la instalación al DSI	

Contingencia: Fallas en el Hardware.

Etapas	**Quien Detecta**	**Responsables**		
		Operador de sistema	**Responsable de Seguridad Informática**	**DSI**
Información	Informa al Responsable de Seguridad Informática			
Neutralización		**PDVAL e Híper-PDVAL**		Se llevaran

		Intentara recuperar la información digitalmente si se tratase de cajas registradoras.	Orienta a la supervisora de cajas que retire las cintas auditoras de las mismas y apague los equipos si se trata de estos equipos. Si se trata de cualquier otro equipamiento informara al DSI	equipos de repuesto para que la instalación continúe sus funciones y los equipos dañados serán retirados para su reparación.
		Oficinas y Almacenes		
		En cualquiera de los casos de equipos de oficinas o comunicaciones estos se apagarán	Informara al DSI	
Recuperación	Realiza las anotaciones en el Registro 1		Informará la finalización de las actividades y la puesta en marcha de la instalación al DSI Relazará los apuntes en los Registros 3 y 7	Relazará los apuntes en el Registro 5

Contingencia: Errores en operaciones del sistema.

Etapas	**Quien Detecta**	**Responsables**	
		Responsable de Seguridad Informática	**DSI**
Información	Informa al Responsable de Seguridad Informática		

Neutralización	Ejecutar las acciones que del DSI le informe al Responsable de la Seguridad Informática	Informar al DSI y esperar instrucciones.	
Recuperación	Realiza las anotaciones en el Registro 1		Restauración de la información, por lo que se utilizará la salva de la Base de Datos

Contingencia: Robo de información o equipamiento.

Etapas	**Quien Detecta**	**Responsables**	
		Responsable de Seguridad Informática	**DSI**

Información	Informa al Responsable de Seguridad Informática		
Neutralización		Orientara la cancelación de todas las operaciones en la instalación y el retiro de todo el personal de los locales. Informara al personal de PCP de la situación de la misma forma informará al DSI. Esperará instrucciones.	En conjunto con la ASI y el personal de PCP de la instalación se coordinaran los procesos de investigación del hecho.
Recuperación	Realiza las anotaciones en el Registro 1	Informará la puesta en marcha de la instalación y la finalización de las investigaciones.	Emitirá un informe completo a la ASI

Contingencia: Filtración de información clasificada entre el personal no autorizado.

Etapas	**Quien Detecta**	**Responsables**		
		Responsable de	**DSI**	**ASI**

		Seguridad Informática		
Información	Informa al Responsable de Seguridad Informática			
Neutralización		Concentrará toda la información sensible que tenga bajo su custodia e informara al DSI.	Concentrará toda la información sensible que tenga bajo su custodia y todos los soportes de la misma. Se cambiaran las claves de las PC.	Se cambiaran las claves de acceso. Y se realizara un catalogo de la información que fue divulgada. Así como una auditoria a los archivos logs del sistema.
Recuperación	Realiza las anotaciones en el Registro 1		Informará la finalización de las investigaciones. Realiza las anotaciones en el Registro 7	Emitirá un informe completo a la Gerencia General. Realiza las anotaciones en el Registro 7

Contingencia: Corrupción o pérdida de información de las cajas registradoras u otro equipo digital.

Etapas	Quien Detecta	Responsables

		Responsable de Seguridad Informática	Operador de sistema	DSI
Información	Informa al Responsable de Seguridad Informática			
Neutralización		Orientara a la supervisora de cajas terminado ya el horario de atención a la población que retire las cintas auditoras y las entregue al operador de sistema, en caso de tratarse de las cajas registradoras. Informara del hecho al DSI.	Realizara manualmente la entrada de la venta por el sistema según las operaciones que indique la cinta auditora, en caso de tratarse de las cajas registradoras.	Realizara la reconfiguración del equipo que este dañado y se le realizaran pruebas, de presentar problemas se retirara y repondrá con otro tan pronto sea posible.
Recuperación	Realiza las anotaciones en el Registro 1 y 3			Realiza las anotaciones en el Registro 5

Contingencia: Incapacitación de los equipos.

Etapas	Quien Detecta	Responsables	
		Responsable de Seguridad Informática	**DSI**
Información	Informa al Responsable de Seguridad Informática		
Neutralización		Este informara al DSI	Se llevara un repuesto para la continuidad de las actividades en la instalación y se procederá al retiro del equipo dañado para su reparación.
Recuperación	Realiza las anotaciones en el Registro 1 y 3	Informará la puesta en marcha de la instalación	Realiza las anotaciones en el Registro 5

Contingencia: Virus informáticos.

Etapas	Quien Detecta	Responsables		
		Operador de sistema	**Responsable de Seguridad Informática**	**DSI**
Información	Informa al Responsable de Seguridad Informática			
Neutralización		Procederá a desinfectar la PC con el producto antivirus instalado en la PC. De no ser posible este informara al Responsable de Seguridad Informática. Apagará la PC	Informara al DSI.	Procederá a aislar el virus. Se intentara desafectar la PC. De no ser posible se retirará y repondrá con otra lo más rápido posible.
Recuperación	Realiza las anotaciones en el Registro 1 y 3		Informará la puesta en marcha de la instalación	Realiza las anotaciones en el Registro 5

Contingencia: Incendios

Etapas	Quien Detecta	Responsables		
		Miembro del personal	Responsable de Seguridad Informática	DSI
Información	Informa a todo el personal que pueda inmediatamente.			
Neutralización	Procederá a extinguir el fuego con el extintor más cercano que tenga, siempre y cuando esto no represente un peligro para su vida.	Procederá a llamar al servicio de bomberos		
Recuperación	Realiza las anotaciones en el Registro 1		Conjuntamente realizaran una cuantificación de daños y un informe completo que será enviado a la Gerencia General y ASI.	

2.11.4 Pruebas y Mantenimientos.

Para poder realizar pruebas al plan de contingencia, ya que en base a los resultados de estas, serán los ajustes que se le harán los ajustes y mantenimientos a dicho plan, se hace de suma importancia que el personal este preparado, por tanto la Gerencia General conjuntamente con los DSI regionales se hará responsable de las siguientes actividades:

Divulgar entre el personal de la empresa el plan de contingencia, ya que este debe ser de conocimiento para todos en la misma.

Realizar reuniones instructivas para los responsables de la seguridad a todos los niveles, se realizara primero el encuentro con el personal de los DSI regionales, y luego cada DSI se encargara de realizar el encuentro con los responsables de la seguridad en su región.

Los principales temas a debatir serán las etapas del plan de seguridad, las amenazas ante las cuales se levantara el plan de contingencia, cuales son las acciones a seguir ante cada contingencia, cuales son las personas a las que hay que movilizar y cuales son sus responsabilidades en cada caso.

En caso de realizarse cambios en el Plan de Contingencia con carácter urgente deberá informarse de inmediato a la parte afectada, por lo que se precisarán cuales son las novedades que se incorporan a lo ya conocido y hacerlo extensivo a todo el personal mediantes propaganda en la empresa o encuentros con los trabajadores.

La manera más fiable para certificar que algo funciona es probándolo en la práctica, por lo que en los simulacros de contingencia será el escenario, para detectar las deficiencias que tenga el plan o si el personal no conoce los procedimientos o los responsables no son capaces de dirigir las acciones. Con estos fines se plantearan los siguientes niveles de prueba:

Cuatrimestralmente se realizarán revisiones de los procedimientos por parte del personal guiados por el responsable de la seguridad en la entidad u oficinas, se realizaran prácticas de las acciones a tomar para cada una de las contingencias, se realizaran llamadas, revisiones de la información, y demás actividades propuestas por el plan, pero sin usar recursos reservados para este tipo de situaciones.

Una vez al año se realizarán pruebas reales de los procedimientos en las que se hará uso de los recursos que fueron destinados para estas actividades.

Estos simulacros no serán ejecutados por todo el personal de forma masiva, las actividades se llevaran a cabo de la siguiente forma será seleccionada una contingencia a la vez y aplicada a un área determinada de la entidad. El responsable de la seguridad será el supervisor de dichas actividades, por lo que deberá informar con antelación al DSI que la instalación a la que pertenece estará en pruebas del plan de contingencia, para evitar falsas alarmas. Sin afectar las actividades de la empresa se designara un personal que será el observador mientras el área en prueba ejecuta las acciones, con el objetivo de detectar pasos que se violen, procedimientos mal ejecutados y demás deficiencias que se detecten, que irán registrándose en un informe. Al concluir el personal que estuvo involucrado es reunido para el análisis y discusión de los acontecimientos durante el simulacro. Y es aquí donde estará la base para el mejoramiento y actualización del plan de contingencia. Una vez terminado el periodo de prueba y registradas todas las deficiencias y anotadas todas las posibles mejoras que se le puedan realizar al plan, el encargado de la seguridad realizara un informa completo de las actividades y resultados, el cual será enviado al DSI para su estudio conjuntamente con los demás informes.

2.12 Conclusión

Mediante las metodologías utilizadas y las se realizó un correcto levantamientos de activos reconocimiento de de amenazas y riesgos asegurando así una adecuada organización de los activos de acuerdo con su prioridad de protección. De la misma forma mediante la metodología aplicada para la confección de las políticas para la seguridad se lograron políticas con la suficiente especificidad y funcionalidad como para ser aplicadas por el personal y mejorar el estado de la seguridad en la empresa. Por otra parte el plan de contingencia logrado asegura mediante su estructura de matriz que durante cada fase de la contingencia haya un responsable o al menos un personal que de una respuesta ante cada suceso.

Se ha logrado la elaboración de un Plan de Seguridad Informática en el cual se establecen principios y requerimientos de seguridad en la empresa PDVAL, de manera que en su primera versión los mismos aseguran por lo menos el comienzo del desarrollo de un proceso de mejora continua de dicho plan. Ya que el mismo proporciona los mecanismos y procedimientos más importantes para una gestión y un proceso de aseguramiento de la seguridad de los activos informáticos en la empresa, por lo que el principal objetivo de este capitulo ha sido logrado, que es la elaboración de un Plan de Seguridad Informática para la empresa PDVAL.

3 Capitulo 3: Validación de la Propuesta de Plan de Seguridad Informática para la empresa PDVAL.

3.1 Introducción

La encuesta fue aplicada a una cantidad de 5 expertos en el tema, así como miembros de grupo de tele-comunicaciones y servidores de de la empresa, por lo que se tiene en cuenta la experiencia en la actividad de seguridad informática, el nivel profesional y el cargo que ocupa dentro de la organización. Para la validación se le hizo llegar a los expertos el plan y la encuesta preparada, para que pudieran realizar su valoración.

3.2 Encuesta

Datos del Especialista encuestado:

Nombre: _____

Especialidad: _____

Tarea que Desempeña: _____

Teléfono: _____

Correo electrónico: _____

Áreas a inspeccionar:

1. Generales
2. Hardware
3. Software

4. Plan de Contingencia

Observación

En la encuesta, califique de 1 a 5, de manera que 1 es la menor calificación y 5 la mayor.

1. Generales

1. ¿El alcance diseñado para el Plan propuesto está bien definido? ____
2. ¿Están definidas las políticas de Seguridad Informáticas?____
3. ¿Se propone que la gerencia tenga pleno conocimiento de las políticas de Seguridad Informáticas y brinde su apoyo a ella?____
4. ¿Las amenazas definidas en el plan y las consecuencias que pueden acarrear ellas, brindan realmente la idea de cuáles son las áreas que se deben chequear constantemente?____
5. ¿La propuesta realizada para el control de los riesgos sobre los activos de la empresa y el orden obtenido para su chequeo y control, se ajusta a las políticas de la empresa? ____
6. ¿La gestión de riesgos presentada en el plan cumple las necesidades requeridas para mantener los activos de la empresa a salvo de daños o dentro del margen aceptable?____

2. Hardware

1. ¿El plan propone la existencia de políticas y procedimientos relativos al uso y protección del hardware? ____
2. ¿Se especifica la debida ubicación física del equipamiento en las instalaciones, para proponer la más adecuada en consecuencia con los diversos desastres o contingencias que se pueden presentar (manifestaciones o huelgas, inundaciones, incendios, otros)?____

3. ¿Se proponen los procedimientos que garanticen la continuidad y disponibilidad de los servidores en caso de desastres o contingencias? ____

4. ¿Se especifica como debe ser el control y procedimientos para la clasificación y justificación del personal con acceso a los servidores? ____

5. ¿Se propone la creación de un grupo con personal de seguridad encargado de la salvaguarda de los equipos de cómputo de la empresa? ____

6. ¿Se proponen políticas relacionadas con el ingreso y salida del hardware que asegure al menos?_____

3. Software

1. ¿El Plan propone la existencia de políticas y procedimientos relativos al uso y protección del software utilizado?____

2. ¿Se proponen procedimientos para comprobar que los totales de los reportes de validación del usuario concuerden con los totales de validación del sistema computarizado?____

3. ¿Se especifica los procedimientos que permitan identificar con claridad las responsabilidades en cuanto al uso del sistema y equipo de cómputo donde será implantado y operado? _____

4. ¿Se propone en el Plan la forma de realizar el respaldo de la información del sistema?____

5. ¿Se especifica los controles para que sólo personal autorizado tenga acceso a dichos respaldos?___

4. Plan de Contingencia

1. ¿El Plan de Contingencia propuesto contempla aspectos tales como: redes de comunicación, hardware, aplicaciones, datos, recursos humanos, lugares físicos donde se encuentran los recursos anteriores y otros?____

2. ¿La propuesta hecha en el análisis de riesgo es efectiva para medir la importancia de los activos de la empresa?___

3. ¿La propuesta del plan de contingencia cubren los procedimientos necesarios para prevenir los elementos causales o restaurar los primordiales?____

4. ¿Se propone el orden en que se reiniciarían las operaciones de la aplicación de acuerdo con las prioridades y estrategias del negocio?____

5. ¿Se presenta una clasificación, para que la operación del sistema no se interrumpa por un desastre o contingencia, de los elementos prioritarios: equipamiento, datos, sistemas operativos, documentación, personal, entre otros?____

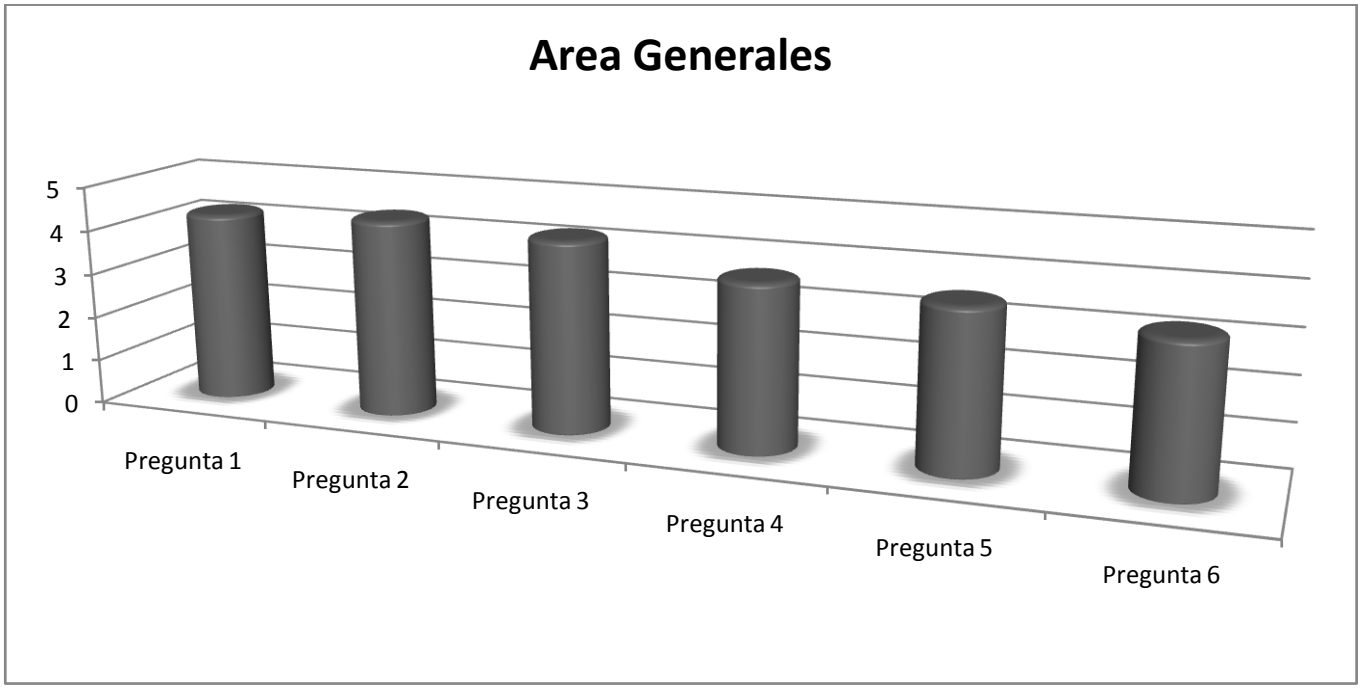
3.3 Resultados arrojados por la encuesta

3.3.1 Área Generales

Los resultados de las preguntas del área Generales se muestran en la tabla a continuación:

Resultados de las preguntas del área Generales

Pregunta 1	Pregunta 2	Pregunta 3	Pregunta 4	Pregunta 5	Pregunta 6
4.28	4.42	4.28	3.71	3.57	3.28



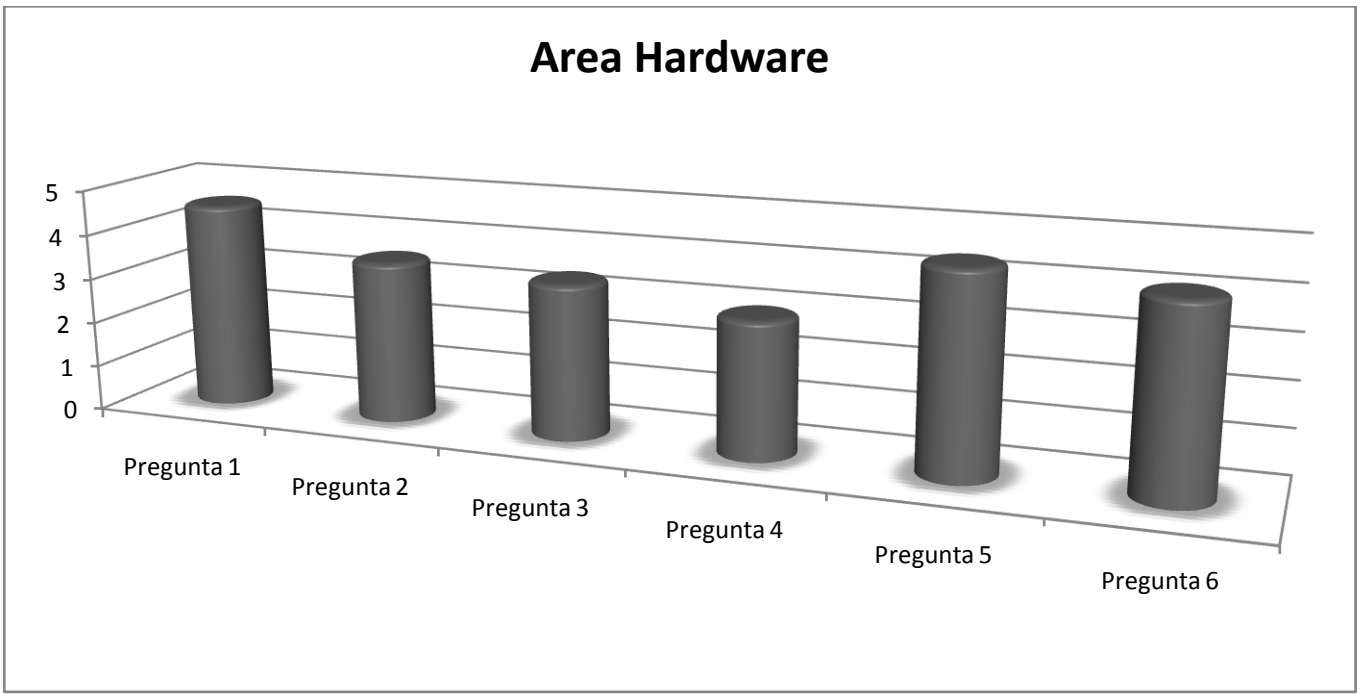
En esta área se refleja una correcta definición del alcance del plan de seguridad, así como la definición de las políticas de seguridad; de igual forma el plan deja establecido que la gerencia deberá tener total conocimiento del desarrollo de la seguridad y brindar el mayor apoyo al personal encargado de la seguridad. Las amenazas identificadas, son aceptables aunque no brindan del todo una total idea de cuales son las amenazas a monitorear con más frecuencia. De igual forma podría mejorarse la propuesta para el control de los riesgos, así como la gestión de los mismos.

3.3.2 Área Hardware

Los resultados de las preguntas del área de Hardware se muestran en la tabla a continuación:

Resultados de las preguntas del área Hardware

Pregunta 1	Pregunta 2	Pregunta 3	Pregunta 4	Pregunta 5	Pregunta 6
4.57	3.57	3.42	3	4.42	4.14



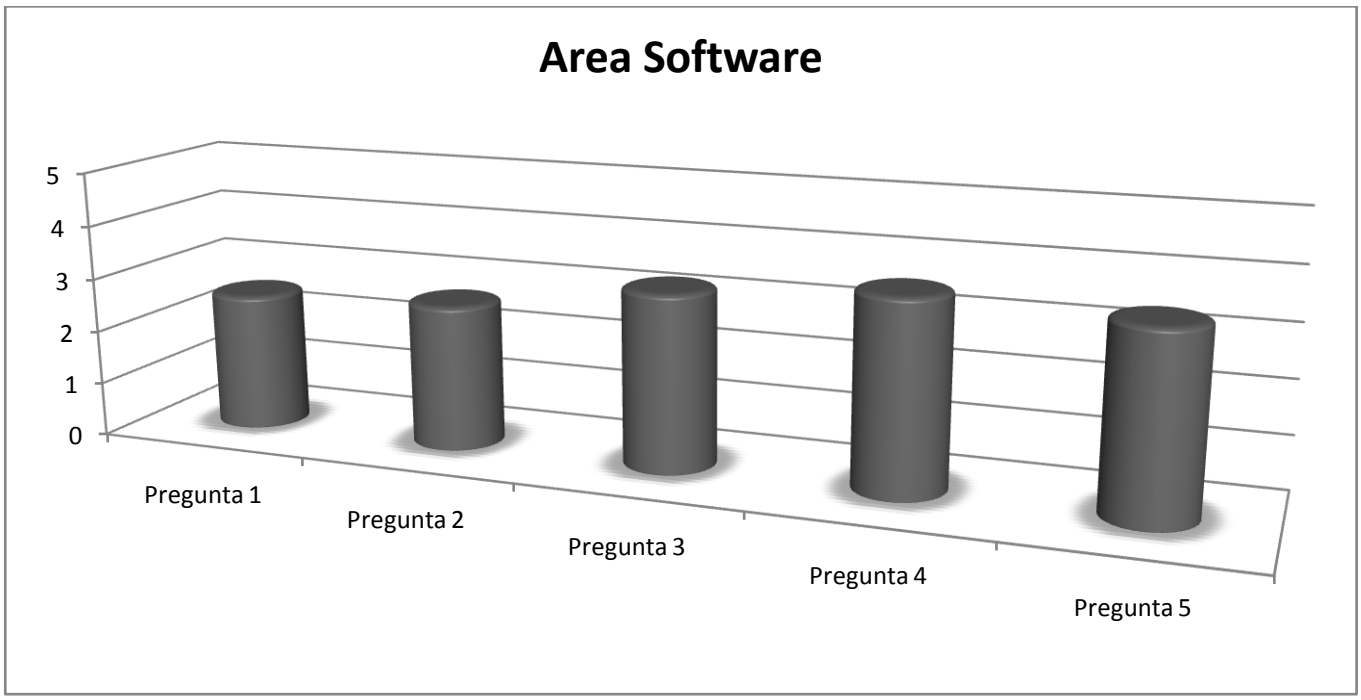
Se confirma que las medidas para la protección relativas al hardware de la empresa fueron precisas e inciden realmente en los problemas en este sentido y actúan sobre ellos. Aunque no se logra una correcta descripción de la ubicación que debería tener cada activo dependiendo de las amenazas que lo asechan; de la misma forma pasa con la descripción de los procedimientos para la continuidad de los procesos de la empresa y la clasificación y justificación del personal que deberá tener acceso a los recursos críticos de la empresa como sus servidores e información sensible. Pero se evidencia un correcto análisis respecto a la creación de grupos de trabajo y de procedimientos de control sobre los activos informáticos, para garantizar la seguridad en la empresa.

3.3.3 Área Software

Los resultados de las preguntas del área de Software se muestran en la tabla a continuación:

Resultados de las preguntas del área Software

Pregunta 1	Pregunta 2	Pregunta 3	Pregunta 4	Pregunta 5
2.57	2.71	3.28	3.57	3.42



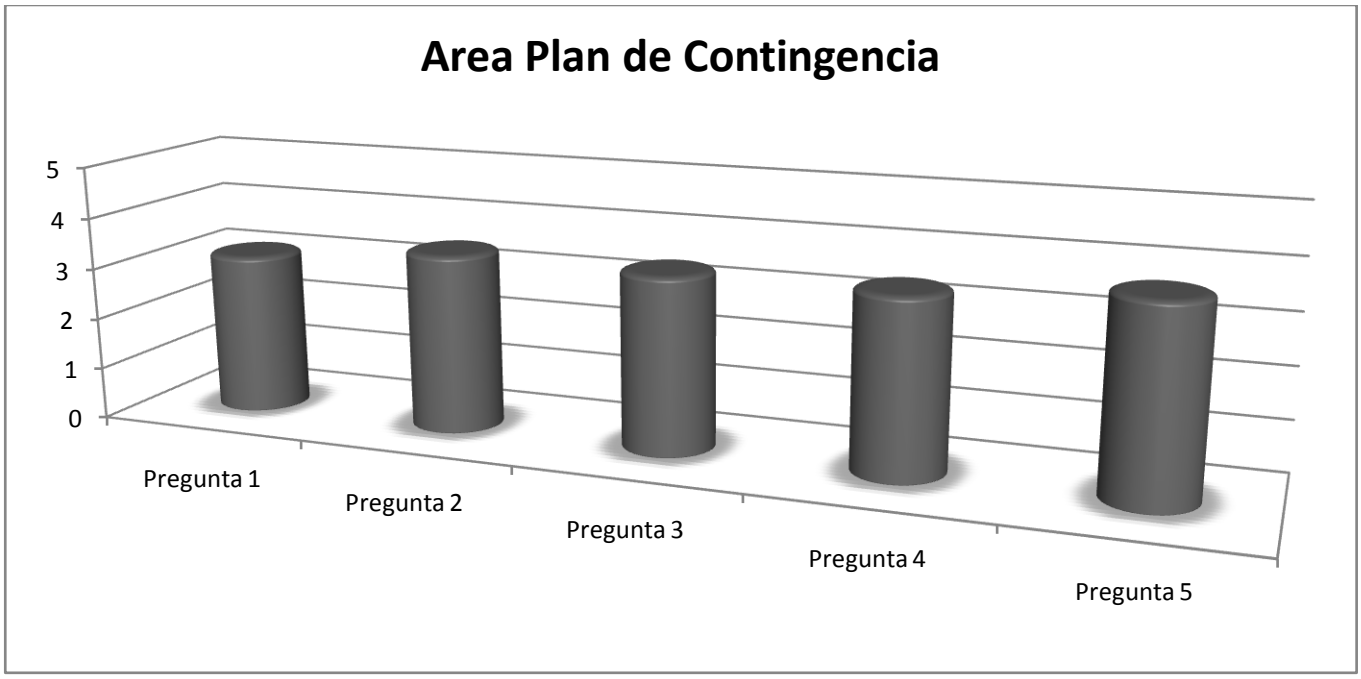
Se evidencia la existencia de políticas y medidas para la protección del software usado por la empresa pero no en la medida requerida por la empresa, así como la validación de los resultados de las ventas y movimientos de mercancía. Las especificidades de selección del personal que trabajará con el equipamiento informático de la empresa no son tratadas con la profundidad suficiente en el plan. Pero si se especifican los pasos y frecuencias de realización de las salvas de la información, así como el personal que tendrá acceso a las mismas.

3.3.4 Área Plan de Contingencia

Los resultados de las preguntas del área de Plan de Contingencia se muestran en la tabla a continuación:

Resultados de las preguntas del área Plan de Contingencia

Pregunta 1	Pregunta 2	Pregunta 3	Pregunta 4	Pregunta 5
3.14	3.48	3.42	3.42	3.71



Según los resultados de la encuesta el plan no detalla lo suficiente el control de los aspectos como: redes de comunicación, hardware, aplicaciones, datos, recursos humanos, etc. De igual forma la propuesta de análisis para establecer la prioridad de protección de los activos, aunque es aceptable no contempla en su totalidad todos los elementos necesarios a tener en cuenta. El plan de contingencia especifica las medidas a tomar en caso de los acontecimientos más relevantes y generales dejando de lado los sucesos menos significativos que pudieran afectar la seguridad de la empresa. Por lo que dicho plan de contingencia es funcional y aplicable, mencionando la necesidad de perfeccionarlo y especificarlo aun más al entorno de la empresa PDVAL.

3.4 Conclusión

El Plan de Seguridad Informática para la empresa PDVAL, fue sometido a la opinión y evaluación de una población seleccionada de 5 expertos en el tema con que cuenta la empresa, personal encargado de las redes y operaciones de la empresa en esta fase inicial. Como objetivo principal dicha encuesta perseguía la obtención de información necesaria para verificar la viabilidad de dicho plan de seguridad.

Los resultados de la evaluación arrojaron que el plan propuesto para la empresa recoge todas los aspectos necesarios dentro de un plan de seguridad en general y estableces las normas que deben cumplir el personal de la organización, así como todos los entes que deben estar controladas para evitar cualquier daño o pérdida de la información, desde el hardware, software y los seres humanos. También fueron detectados puntos débiles dentro del plan los cuales fueron resaltados por los expertos, dentro de ellos encontramos:

1. Las amenazas identificadas, son aceptables aunque no brindan del todo una total idea de cuales son las amenazas a monitorear con más frecuencia.

2. De igual forma podría mejorarse la propuesta para el control de los riesgos, así como la gestión de los mismos.

3. Las especificidades de selección del personal que trabajará con el equipamiento informático de la empresa no son tratadas con la profundidad suficiente en el plan.

4. La propuesta de análisis para establecer la prioridad de protección de los activos, aunque es aceptable no contempla en su totalidad todos los elementos necesarios a tener en cuenta.

4 Conclusiones

El estudio e investigación de las metodologías para el desarrollo de planes de seguridad informática, análisis de riesgos, elaboración de políticas para la seguridad y la confección de planes de contingencia, dotaron del conocimiento necesario para poder realizar el análisis pertinente en la empresa y crear las bases para la obtención de plan de seguridad informática desarrollado.

La elaboración de la propuesta de plan de seguridad informática para la empresa PDVAL, fue llevada a cabo con éxito, ofreciendo las bases para la perfección y elaboración de futuros planes.

Dicho plan fue propuesto y sometido al criterio de los expertos en el tema de la organización, dando como resultado que el mismo era funcional y aplicable, con el señalamiento de que algunas áreas de la propuesta desarrollada no se acerca lo suficiente a las especificaciones de la empresa, áreas que pueden rectificarse en próximas presentaciones del plan, acercándolo más al entorno de la empresa PDVAL.

5 Recomendaciones

Producto a los resultados arrojados por la encuesta realizada a los especialistas en el tema, surgieron aspectos importantes, los cuales deberían solucionarse para la puesta en uso del plan, estos aspectos son:

1. Mejora de la propuesta para el control de los riesgos, así como la gestión de los mismos.
2. Elaborar unas plantillas donde se recojan las especificidades de selección del personal que trabajará con el equipamiento informático de la empresa, para un control más efectivo.
3. Refinar la propuesta de análisis para establecer la prioridad de protección de los activos, ya que aunque aceptable, no contempla en su totalidad todos los elementos.
4. Se recomienda tras refinar el plan de seguridad informática propuesto, su inmediata aplicación en la organización en aras de proteger todos los aspectos, que pudieran atentar contra la pérdida o robo de la información, software, hardware y recursos humanos.

6 Bibliografía

Holbrook, J. Paul and Reynolds, Joyce K. Site Security Handbook.

ISO. 2005. Estandar Internacional ISO/IEC 17799 , Tecnología de la Información – Técnicas de seguridad – Código para la práctica de la gestión de la seguridad de la información. 2005.

Lizama Mendoza, Jorge Alberto. 2005. *HACKERS EN EL CONTEXTO DE LA SOCIEDAD DE LA INFORMACIÓN.* Mexico D.F : s.n., 2005.

Martos Sanquillo, Alberto. 2001. Instrucciones y ejemplos para hacer un Plan de Seguridad Informático. Colombia : s.n., 2001.

Mora Marín, Guillermo. 2006. Sevilla : s.n., 2006.

Sánchez Marín, Jose Ignacio, Gorrotxategi Zurimendi, Gorka and Garaizar Sagarminaga, Pablo. Seguridad Informática.

Swanson, Marianne, Hash, Joan and Bowen, Pauline. 2006. Guide for Developing Security Plans for Federal Information Systems. 2006.

Taller de Desarrollo de Políticas de Seguridad. **Núñez Sandoval, Alejandro. 2005.** Mexico D.F. : s.n., 2005.

Untiveros, Sergio. 2004. Metodologías para administradores de redes. 2004.

[Eje Seguridad Informática] Proyecto SOMAP.org. **Rosso, Leonardo. 2007.** Buenos Aires : s.n., 2007.

Arce, Iván. Tendencia en ataques Informáticos. Buenos Aires : s.n.

Berenguela Castro, Alfonso Antonio and Cortes Collado, Juan Pablo. 2006. *METODOLOGÍA DE MEDICIÓN DE VULNERABILIDADES EN REDES DE DATOS DE ORGANIZACIONES.* Stg. de Chile : s.n., 2006.

Bisogno, María Victoria. Elaboración del Plan de Recuperación de Desastres (PRD). Buenos Aires : s.n.

Bibliografía

Borghello, Cristian Fabian. 2001. *Seguridad Informática sus Implicancias e Implementación.* Buenos Aires : s.n., 2001.

Cepeda González, Fausto. 2008. Mejores Prácticas para Proteger Información Corporativa. Mexico D.F. : s.n., 2008.

CISCO . A Beginner's Guide to Network Security.

Comunicaciones, Universidad Nacional de Colombia Vicerrectoría General Dirección Nacional de Informática y. 2003. Guia para elaboración de políticas de Seguridad. 2003.

Córdova Rodríguez, Norma Edith. Plan de Seguridad Informática para una Entidad Financiera.

Ferrer, Rodrigo. Metodología de Análisis de Riesgo. Bogotá : s.n.

Franco, Alfonso Gómez. 2004. Análisis de Conseptos Auditoria de seguridad. 2004.

Gestion de la seguridad de la informacion UNE 17502-ISO 17799. **Villalón Huerta, Antonio. 2004.** Valencia : s.n., 2004.

Grupo de Trabajo sobre Seguridad de la Información y Privacidad (GTSIP). GUÍAS DE LA OCDE PARA LA SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN Y REDES.

Hernández León, Rolando Alfredo and Coello González, Sayda. 2002. *EL PARADIGMA CUANTITATIVO DE LA INVESTIGACIÓN CIENTIFICA.* Cuidad de la Habana : EDUNIV, 2002.

[Online] http://www.iso1799.com/.

[Online] http://www.symantec.com/region/mx/enterprisesecurity.

[Online] http://www.uaslp.mx/PDF/2042_182.pdf..

[Online] http://www.mastermagazine.info/termino.

[Online] http://www.asesoriainformatica.com/definiciones_i.htm.

[Online] http://www.delitosinformaticos.com/11/2006/seguridad-informatica/analisis-iso-270012005.

7 Anexos

Anexo #1: Plantilla para la elaboración del plan.

1. Introducción <*breve explicación sobre el plan*>
2. Objetivos <*que se persigue con la implementación de este plan*>
3. Alcance <*hasta donde y hasta quienes estará dirigido el plan*>
4. Definiciones <*definiciones técnicas, conceptos, explicación de siglas, etc.*>
5. Caracterización <*explicación de la situación actual de la organización*>
   5.1 Aplicaciones en explotación <*cuales son las aplicaciones que están en uso por la organización*>
6. Estructuras de Gestión de la Seguridad Informática <*como se va organizar la gestión de la seguridad a manera de equipos de trabajo*>
   6.1 Responsabilidades <*cuales serán las responsabilidades de estos equipos*>
   6.2 Los roles <*definir los roles de los equipos y sus obligaciones*>
   6.3 Control de la Seguridad en las instalaciones <*la distribución de roles según los locales de la organización*>
   6.4 Responsabilidades en las instalaciones <*cuales serán las funciones de los roles en cada una de las instalaciones o locales de la organización*>
7. Gestión de Riesgos <*desarrollo del proceso de identificación, análisis y estimación de riesgos*>
   7.1 Los activos

Descripción	**Tipo**	**Ubicación**
<Nombre, modelo, marca>	<Tipo de activo>	<Lugar donde está ubicado>

Tabla. Relación de activos, tipo y ubicación.

   7.2 El equipamiento
   7.3 Importancia de activos

Activo	**Parámetros** <se colocan tantas columnas como parámetros a tener en cuenta>					**Importancia (Wi)** <resultado del promedio de parámetros>
	Función	**Costo**	**Confidencialidad**	**Integridad**	**Disponibilidad**	
<Descripción de activos>	#	#	#	#	#	#

Tabla. Importancia de activos informáticos.

Activo <descripción del activo>	**Importancia (Wi)** <valor resultante organizado descendentemente>

Tabla. Activos por orden de importancia

7.4 Amenazas

7.5 Consecuencias

Amenaza <descripción de la amenaza>	**Consecuencias** <consecuencias que acarrea la amenaza>

Tabla. Consecuencias de las amenazas en caso de que ocurriesen.

7.6 Estimación de Riesgos *<cuales son los activos más valiosos y cuales requieren mayor atención>*

Activo <Descripción de activos>	**Amenazas**							**Ri**	**Wi**	**Pi**
	1	2	3	4	5	6	…			

Tabla. Cálculo de prioridad de protección de los activos informáticos.

Activo	**Prioridad**
<descripción de activos>	<resultado de la tabla anterior>

Tabla #8. Relación de activos por Prioridad

8. Sistema de Medidas para la Seguridad Informática <las políticas para la seguridad agrupadas según las categorías siguientes>.
   - 8.1 Medidas administrativas y organizativas
   - 8.2 Medidas respecto a la información
     - 8.2.1 Soportes de información
     - 8.2.2 Conservación
     - 8.2.3 Destrucción
     - 8.2.4 Traslado
   - 8.3 Clasificación de la Información
   - 8.4 Medidas respecto al personal
   - 8.5 Medidas de seguridad Física
     - 8.5.1 Áreas a proteger
     - 8.5.2 Barreras Físicas
     - 8.5.3 Mecanismos de protección Física aplicados
     - 8.5.4 Control de Acceso a las Tecnologías de la información
     - 8.5.5 Sistema de control de Acceso
   - 8.6 Medidas de seguridad Lógica
     - 8.6.1 Protección de acceso a las Tecnologías de Información
     - 8.6.2 Identificación y Autenticación de Usuarios
     - 8.6.3 Claves
     - 8.6.4 Traza de auditoria sobre acciones que amenazan la seguridad
     - 8.6.5 Protección contra programas dañinos
     - 8.6.6 Control de acceso
   - 8.7 Medidas de Seguridad de Operaciones
     - 8.7.1 Salvas
     - 8.7.2 Mantenimiento y reparación de medios técnicos
     - 8.7.3 Control del uso, traslado y entrada de tecnologías de información

Anexo #2. Etiqueta de Soporte de Información.

No. Soporte:	Categoría:
Descripción:	

Anexo #3.

Acta de Destrucción de Información

Por carecer de importancia y valor funcional para la empresa la información contenida en el soporte con Número _____, Clasificada como _____. Es destruida hoy ___, del mes de _____ del año _____, mediante _____.

Con la autorización de

Nombre: _____ Firma: _____

Y en la presencia de

Cuño_____

Anexo #4

Autorización de Entrada-Salida de las Equipamiento Informático

Fecha: Hora: __Entrada __Salida

Equipos Modelo Serial

Quien realiza el traslado: _____

Autoriza: _____ Firma: _____

Anexo # 5: Registro No. 1 Incidencia de la Seguridad Informática

Registro 1	**Incidencias de la Seguridad Informática**				
Ubicación: <Nombre de la instalación, departamento, oficina o ubicación del local>					
No.	**fecha**	**hora**	**Solapín**	**Nombre y apellidos**	**área**
Hecho detectado					

Anexo # 6: Registro No. 2 Uso de Soportes de Información

Registro 2	**Uso de Soportes de Información**						
Ubicación: <Nombre de la instalación, departamento, oficina o ubicación del local>							
No.	**Solapín**	**Nombre y Apellidos**	**Cód. Soporte**	**inicio**		**fin**	
				fecha	**hora**	**fecha**	**hora**
Actividades realizadas							

Anexo #7: Registro No. 3 Entrada-Salida y Movimiento de Equipamiento

<table>
<tr><td colspan="2">Registro 3</td><td colspan="5">Entrada-Salida y Movimiento de Equipamiento</td></tr>
<tr><td colspan="7">Ubicación: <Nombre de la instalación, departamento, oficina o ubicación del local></td></tr>
<tr><td>fecha</td><td>hora</td><td>Procedencia</td><td>Destino</td><td colspan="2">Nombre y Apellidos</td><td>Firma</td></tr>
<tr><td colspan="3">Marca</td><td colspan="4" rowspan="3">Motivos del movimiento</td></tr>
<tr><td colspan="3">Modelo</td></tr>
<tr><td colspan="3">Serial</td></tr>
<tr><td colspan="7">Observaciones</td></tr>
</table>

Anexo # 8: Registro No. 4 Registro de Acceso

<table>
<tr><td colspan="2">Registro 4</td><td colspan="3">Registro de Acceso</td></tr>
<tr><td colspan="5">Ubicación: <Nombre de la instalación, departamento, oficina o ubicación del local></td></tr>
<tr><td colspan="2">Fecha</td><td rowspan="2">Visitante</td><td colspan="2" rowspan="2">Solapín/ Cédula</td></tr>
<tr><td>Ent.</td><td>Sal.</td></tr>
<tr><td colspan="2" rowspan="2"></td><td>Autoriza</td><td colspan="2">Solapín</td></tr>
<tr><td colspan="5">Área:
Motivo del acceso:</td></tr>
</table>

Anexo # 9: Registro No. 5 Mantenimiento de Equipamiento

<table>
<tr><td>Registro 5</td><td colspan="2">Mantenimiento de Equipos</td></tr>
<tr><td colspan="3">Ubicación: <Nombre de la instalación, departamento, oficina o ubicación del local></td></tr>
<tr><td>fecha</td><td>Solapín</td><td>Nombre y Apellidos</td></tr>
<tr><td colspan="2">Marca</td><td rowspan="3">Trabajos realizados</td></tr>
<tr><td colspan="2">Modelo</td></tr>
<tr><td colspan="2">Serial</td></tr>
<tr><td colspan="3">Observaciones</td></tr>
</table>

Anexo # 10: Registro No. 6 Control de Soportes

<table>
<tr><td>Registro 6</td><td colspan="2">Control de Soportes</td></tr>
<tr><td colspan="3">Ubicación: <Nombre de la instalación, departamento, oficina o ubicación del local></td></tr>
<tr><td>Número/Serial</td><td>Contenido</td><td>Clasificación</td></tr>
<tr><td>Fecha ingreso</td><td colspan="2" rowspan="2">Observaciones</td></tr>
<tr><td>Fecha de baja

Motivo</td></tr>
</table>

Anexo # 11: Registro No. 7 Entrega-Recepción de Soportes

Registro 7	**Entrega-Recepción de Soportes**		
Ubicación: <Nombre de la instalación, departamento, oficina o ubicación del local>			
No.	**Número/Serial**		
Entrega	**Fecha:**	**Hora:**	
Nombre y apellidos (entrega)		**Solapín**	**Firma**
Nombre y apellidos (recibe)		**Solapín**	**Firma**
Recepción	**Fecha:**	**Hora:**	
Nombre y apellidos (devuelve)		**Solapín**	**Firma**
Nombre y apellidos (recibe)		**Solapín**	**Firma**
Resultado de chequeo de lista de nombres			
Resultado de escaneo de virus			
Observaciones			

Anexo # 12: Registro No. 8 Registro de Inspecciones

Registro 8	**Registro de Inspecciones**		
Fecha	**Instalación objeto de la inspección**	**Área**	
Responsable de la inspección		**Solapín**	**Firma**
Participantes			
Deficiencias detectadas			
Plan de medidas			
Evaluación de la inspección			
Observaciones			

Anexo # 13: Encuesta para la validación del Plan de Seguridad Informática propuesto para la empresa PDVAL

Datos del Especialista encuestado:

Nombre: _____

Especialidad: _____

Tarea que Desempeña: _____

Teléfono: _____

Correo electrónico: _____

Áreas a inspeccionar:

1. Generales
2. Hardware
3. Software
4. Plan de Contingencia

Observación

En la encuesta, califique de 1 a 5, de manera que 1 es la menor calificación y 5 la mayor.

1. <u>Generales</u>

1. ¿El alcance diseñado para el Plan propuesto está bien definido? ____
2. ¿Están definidas las políticas de Seguridad Informáticas?____
3. ¿Se propone que la gerencia tenga pleno conocimiento de las políticas de Seguridad Informáticas y brinde su apoyo a ella?____

4. ¿Las amenazas definidas en el plan y las consecuencias que pueden acarrear ellas, brindan realmente la idea de cuáles son las áreas que se deben chequear constantemente?____

5. ¿La propuesta realizada para el control de los riesgos sobre los activos de la empresa y el orden obtenido para su chequeo y control, se ajusta a las políticas de la empresa? ____

6. ¿La gestión de riesgos presentada en el plan cumple las necesidades requeridas para mantener los activos de la empresa a salvo de daños o dentro del margen aceptable?____

2. Hardware

1. ¿El plan propone la existencia de políticas y procedimientos relativos al uso y protección del hardware? ____

2. ¿Se especifica la debida ubicación física del equipamiento en las instalaciones, para proponer la más adecuada en consecuencia con los diversos desastres o contingencias que se pueden presentar (manifestaciones o huelgas, inundaciones, incendios, otros)?____

3. ¿Se proponen los procedimientos que garanticen la continuidad y disponibilidad de los servidores en caso de desastres o contingencias? ____

4. ¿Se especifica como debe ser el control y procedimientos para la clasificación y justificación del personal con acceso a los servidores? ____

5. ¿Se propone la creación de un grupo con personal de seguridad encargado de la salvaguarda de los equipos de cómputo de la empresa? ____

6. ¿Se proponen políticas relacionadas con el ingreso y salida del hardware que asegure al menos?_____

3. Software

1. ¿El Plan propone la existencia de políticas y procedimientos relativos al uso y protección del software utilizado?____

2. ¿Se proponen procedimientos para comprobar que los totales de los reportes de validación del usuario concuerden con los totales de validación del sistema computarizado?____

3. ¿Se especifica los procedimientos que permitan identificar con claridad las responsabilidades en cuanto al uso del sistema y equipo de cómputo donde será implantado y operado? _____
4. ¿Se propone en el Plan la forma de realizar el respaldo de la información del sistema?____
5. ¿Se especifica los controles para que sólo personal autorizado tenga acceso a dichos respaldos? ___

4. <u>Plan de Contingencia</u>

1. ¿El Plan de Contingencia propuesto contempla aspectos tales como: redes de comunicación, hardware, aplicaciones, datos, recursos humanos, lugares físicos donde se encuentran los recursos anteriores y otros?____
2. ¿La propuesta hecha en el análisis de riesgo es efectiva para medir la importancia de los activos de la empresa?___
3. ¿La propuesta del plan de contingencia cubren los procedimientos necesarios para prevenir los elementos causales o restaurar los primordiales?____
4. ¿Se propone el orden en que se reiniciarían las operaciones de la aplicación de acuerdo con las prioridades y estrategias del negocio?____
5. ¿Se presenta una clasificación, para que la operación del sistema no se interrumpa por un desastre o contingencia, de los elementos prioritarios: equipamiento, datos, sistemas operativos, documentación, personal, entre otros?____