UNIVERSIDAD DEL AZUAY

FACULTAD DE CIENCIAS DE LA ADMINISTRACIÓN

ESCUELA DE ANÁLISIS INFORMÁTICO

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN APLICADAS A UNA RED LOCAL DE CIBERCAFÉ

Trabajo de monografía previo a la obtención del título de

Analista en Informática

Autor: Mónica Jara Peña

Director: Ing. Esteban Crespo Martínez

Cuenca, Ecuador

2011

DEDICATORIA

A mis hijos Paulina, Pablo y Ariana y a mi esposo

quienes son la razón de mi vivir.

AGRADECIMIENTOS

- A mi familia por el apoyo y comprensión que siempre me brindan.
- Un especial reconocimiento a mi guía, apoyo y ejemplo, en el transcurso del curso de graduación y en la elaboración de esta monografía, Máster Esteban Crespo Martínez, por creer siempre en mi trabajo y por la confianza y conocimientos que me ha transmitido.
- A todo el personal docente y administrativo de la Universidad del Azuay por la ayuda brindada para la culminación de este trabajo.

Mónica

INDICE DE CONTENIDOS

RESUMEN

Las Políticas de Seguridad de la Información aplicadas a una red local de un Cibercafé, es un modelo de Sistema de Gestión de la Seguridad de la Información (SGSI), para empresas o negocios similares, dentro de la realidad actual del país.

Con este fin, se realizó un análisis teórico y práctico para la implementación de políticas de seguridad de la información basadas en las Normas ISO 27001. Además de evaluar herramientas de control y software libre (GNU) como: Elistara, Superantispyware o SpyBoot, Kaspersky Internet Security y GFI LanGuard Network Scanner, para garantizar la confidencialidad, integridad y disponibilidad de la información.

Mónica Jara Peña

ABSTRACT

The Information Security Policy applied to a local network in a Cybercafé, is a model of an Information Security Management System (ISMS) for similar enterprises or businesses within the country's current situation.

For this reason, a theoretical and practical analysis for the implementation of security policies was carried out based on the ISO 27001 regulations. In addition, control tools and free software (GNU) such as: Elistara, Superantispyware or SpyBoot, Kaspersky Internet Security and GFI LanGuard Network Scanner, were evaluated in order to guarantee the information's confidentiality, integrity and availability.

UNIVERSIDAD DEL AZUAY
DPTO. IDIOMAS

Translated by,

Diana Lee Rodas

CAPITULO I

GENERALIDADES

1.1 ANTECEDENTES.

En el contexto actual mundial y local, no podemos desconocer la importancia y la influencia de la red interconectada más grande del mundo, conocida como Internet. El Internet, como se lo conoce en nuestro medio, se ha convertido en una herramienta básica para la mayoría de empresas, estudiantes y personas de todo género e índole.

Es a través de esta red, que manejamos un sinnúmero de información de carácter personal, empresarial, comercial, social, etc., realizamos negocios, pagos, adquirimos bienes y servicios, consultamos precios, proveedores, clientes, etc.; y es precisamente esta utilidad, la que en la actualidad se ha convertido en un blanco de ataques, debido, por un lado, a la diversidad y heterogeneidad de los sistemas de información que utilizan las empresas, y por otro, a la globalización a la que se ven enfrentadas al tener que conectar estos sistemas de información al Internet, generando un vacio en lo referente a la Seguridad de la Información.

No hace muchos años, aún era considerado un asunto de ciencia ficción, el hablar de suplantación de identidades, robo de información vital de una empresa (clientes, proveedores), robo de dinero a través de cajeros automáticos y tarjetas de crédito, etc., panorama que en la actualidad se ha convertido en una realidad tangible y para la cual la mayoría de empresas, negocios y personas tienen y deben estar preparadas.

Diariamente, en todo el mundo, las computadoras, llámense servidores, estaciones de trabajo o simplemente PC's, son violados y con ello la información de sus usuarios. Esta información puede ser de diversa índole como: las finanzas de la empresa, números de tarjetas de crédito, planes estratégicos, información relacionada con la investigación y el desarrollo de nuevos productos o servicios, etc.

Entre las posibles causas más comunes de estas violaciones a la seguridad de los sistemas de información se encuentran: los defectos potenciales de seguridad en la instalación del software, en la configuración de los servicios de red, "huecos" típicos en las utilerías del sistema operativo y demás software base o de red, así como en la implantación de decisiones administrativas ignorantes de las condiciones mínimas de seguridad para los sistemas.

Estos ataques a los sistemas de información pueden tener diversos fines como: económicos, por tipo de información, para sabotear las operaciones de una empresa, para dañar el prestigio de una empresa, por revanchismo o simplemente por curiosidad, entre otras muchas causas. En cualquier caso, el riesgo e impacto son altos para las empresas. La pérdida de información sensitiva, fraude, paro de operaciones, además de las pérdidas en imagen por el impacto publicitario que genere el ataque, representan altos costos para la empresa.

Es ante esta realidad que debemos hablar de Seguridad Informática y Seguridad de la Información, términos que en ocasiones son utilizados como sinónimos pero que a continuación detallaremos sus deferencias:

El término Seguridad Informática, nace aproximadamente en 1980, con Jame P. Anderson, quien sienta las bases de lo que hoy se conoce con el tema de Seguridad Informática, con el documento "Computer Security Threat Monitoring and Surveillance".
(Tomado de http://blogs.technet.com/b/ponicke/archive/2007/04/19/seguridad-informatica-un-poco-de-historia.aspx, 05-05-2011)

La Enciclopedia libre Wikipedia (http://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica,05-05-2011) define y hace una diferenciación entre los términos Seguridad Informática y Seguridad de la Información:

> "La **seguridad informática** es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta (incluyendo la información contenida). Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La seguridad informática comprende software, bases de datos, metadatos, archivos y todo lo que la organización valore (activo) y signifique un riesgo si ésta llega a manos de otras personas. Este tipo de información se conoce como información privilegiada o confidencial."

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

En estas definiciones se puede observar que el campo de aplicación de la Seguridad Informática es más específico, mientras que la Seguridad de la Información es más general ya que no solo le limita a un solo medio, sin embargo persiguen un mismo fin, proteger la **Confidencialidad**, **Integridad** y **Disponibilidad** de la información.

En este punto es importante conocer algunas definiciones relacionadas con el tema como:

- **Información Critica**: Es indispensable para la operación de la empresa.
- **Información Valiosa**: Es un activo de la empresa y muy valioso.
- **Información Sensitiva**: Debe de ser conocida por las personas autorizadas.
- **Riesgo**: Es todo tipo de vulnerabilidades, amenazas que pueden ocurrir sin previo aviso y producir.
- **Seguridad**: Es una forma de protección contra los riesgos.
- **Confidencialidad:** La confidencialidad es la propiedad de prevenir la divulgación de información a personas o sistemas no autorizados.
- **Integridad:** es la propiedad que busca mantener los datos libres de modificaciones no autorizadas.
- **Disponibilidad:** es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.

- **Auditabilidad:** Permitir la reconstrucción, revisión y análisis de la secuencia de eventos.
- **Identificación:** verificación de una persona o cosa; reconocimiento.
- **Autenticación:** Proporcionar una prueba de identidad; puede ser algo que se sabe, que se es, se tiene o una combinación de todas.
- **Autorización:** Lo que se permite cuando se ha otorgado acceso.
- **No repudio:** no se puede negar un evento o una transacción.
- **Seguridad en capas:** La defensa a profundidad que contenga la inestabilidad.
- **Control de Acceso:** limitar el acceso autorizado solo a entidades autenticadas.
- **Métricas de Seguridad, Monitoreo:** Medición de actividades de seguridad
- **Gobierno:** proporcionar control y dirección a las actividades.
- **Estrategia:** los pasos que se requieren para alcanzar un objetivo.
- **Arquitectura:** el diseño de la estructura y las relaciones de sus elementos.
- **Gerencia:** Vigilar las actividades para garantizar que se alcancen los objetivos
- **Riesgo:** la explotación de una vulnerabilidad por parte de una amenaza.
- **Exposiciones:** Áreas que son vulnerables a un impacto por parte de una amenaza.
- **Vulnerabilidades:** deficiencias que pueden ser explotadas por amenazas.
- **Amenazas:** Cualquier acción o evento que puede ocasionar consecuencias adversas.
- **Riesgo residual:** El riesgo que permanece después de que se han implementado contra medidas y controles.
- **Impacto:** los resultados y consecuencias de que se materialice un riesgo.
- **Criticidad:** La importancia que tiene un recurso para el negocio.
- **Sensibilidad:** el nivel de impacto que tendría una divulgación no autorizada.
- **Análisis de impacto al negocio:** evaluar los resultados y las consecuencias de la inestabilidad.
- **Controles:** Cualquier acción o proceso que se utiliza para mitigar el riesgo.
- **Contra medidas:** Cualquier acción o proceso que reduce la vulnerabilidad.
- **Políticas:** declaración de alto nivel sobre la intención y la dirección de la gerencia.
- **Normas:** Establecer los límites permisibles de acciones y procesos para cumplir con las políticas.

- **Ataques:** tipos y naturaleza de inestabilidad en la seguridad.
- **Clasificación de datos:** El proceso de determinar la sensibilidad y Criticidad de la información.

La Seguridad de la Información también abarca la implementación de estrategias cuyo objetivo primordial es establecer políticas, controles de seguridad, tecnologías y procedimientos para detectar amenazas que puedan encontrar vulnerabilidades y así proteger la información, así como los sistemas que la administran y almacenan.

La Seguridad de la Información es un proceso dinámico, debido a que debe actualizar de forma constante sus políticas y controles, revisarse y adecuarse si es necesario. Una eficaz Gestión de la Seguridad de la Información establece y mantiene programas, establece políticas y controles para conservar la confidencialidad, integridad y disponibilidad de la información (principios básicos de la seguridad de la información), conoce las vulnerabilidades y amenazas, considera las causas de riesgo y la probabilidad de que ocurran, así como su impacto.

Entonces al hablar de una adecuada gestión de la información dentro del área informática, es decir; una adecuada gestión de la Seguridad Informática debemos abordar 2 clases de ámbitos: Seguridad Física y Seguridad lógica.

La Seguridad Física hace referencia a la implementación de barreras físicas y procedimientos de control ante las amenazas que puedan presentarse en el área física, conocida como centro de cómputo donde se encuentran equipos (servidores) con software vital para el normal desarrollo de una empresa o negocio. Protege el hardware de la empresa y los medios de almacenamiento.

Al hablar de amenazas podemos señalar que existen 2 tipos que deben ser considerados en una implementación de políticas de seguridad:

1.- Desastres naturales como incendios, tormentas eléctricas, inundaciones, entre otras.

2.- Desastres ocasionados por el hombre como disturbios, sabotaje, fraude, entre otros.

Luego de considerar las posibles amenazas que debemos detectar y prevenir es importante tomar en consideración las medidas y/o controles a implementarse, como:

1. Control de acceso.
2. Definición de áreas de seguridad.
3. Protección de datos, entre otras que detallaremos más adelante.

Por otro lado, la Seguridad Lógica hace referencia a los daños que puede sufrir la información almacenada, su objetivo primordial es proteger el activo más importante de una empresa o negocio, su información, a través de la implementación de procedimientos y controles que limiten el acceso a los datos únicamente al personal autorizado.

Entre estos procedimientos y controles podemos señalar:

> "1.- Restringir el acceso a los programas y archivos.
>
> 2.- Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.
>
> 3.- Asegurar que se estén utilizados los datos, archivos y programas correctos en y por el procedimiento correcto.
>
> 4.- Que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y no a otro.
>
> 5.- Que la información recibida sea la misma que ha sido transmitida.
>
> 6.- Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.
>
> 7.- Que se disponga de pasos alternativos de emergencia para la transmisión de información. "
>
> (Tomado de: http://www.segu-info.com.ar/logica/seguridadlogica.htm)

Al hablar de control de acceso podemos indicar que existen controles sobre el Sistema Operativo, sobre el software de aplicación, sobre programas utilitarios, entre otros, con la finalidad de proteger la integridad de la información por medio de la creación de accesos restringidos para los usuarios y procesos. Es decir el establecimiento de permisos de acceso, mismos que están regulados por estándares internacionales como el TCSEC Orange Book, ITSEC/ITSEM (europeos) o ISO/ IEC (internacionales) A continuación detallamos algunos requisitos mínimos de seguridad.

- Identificación y autentificación.
- Roles.
- Transacciones.
- Limitaciones a los servicios.
- Modalidad de acceso.
- Ubicación y horario.
- Control de acceso interno.
- Control de acceso externo.
- Administración.

Para finalizar, la Seguridad de un sistema informático debe estar plasmada en una Política de Seguridad de la Información que tomando en consideración los aspectos tratados anteriormente, busque, planifique, conozca, identifique los posibles riesgos, ataques o vulnerabilidades que tiene el manejo de la información y plantee estrategias claras con la finalidad de guiar el manejo de la información para garantizar su seguridad en un contexto complejo de negocios como lo es el actual.

1.2 JUSTIFICACIÓN.

El incremento de ataques a través de Internet en estos últimos 10 años, ha puesto en alerta a la mayoría de usuarios, empresas, negocios e incluso naciones, como lo indica un artículo publicado por la BBC en su sitio web "En el primer semestre de 2002, las compañías conectadas a la internet registraron violaciones de sus sistemas a un ritmo promedio de 32 veces por semana. En la segunda mitad de 2001, esa cifra era de 25…" (http://news.bbc.co.uk/hi/spanish/science/newsid_2431000/2431467.stm).

Tanto es así que en la actualidad se habla de una guerra por el control y manejo de la información a través de Internet, debido a que se ha convertido en un canal por el cual se perpetran ataques que han ocasionado pérdidas de información no sólo a las empresas y negocios de diversos tamaños, sino también a personas naturales.

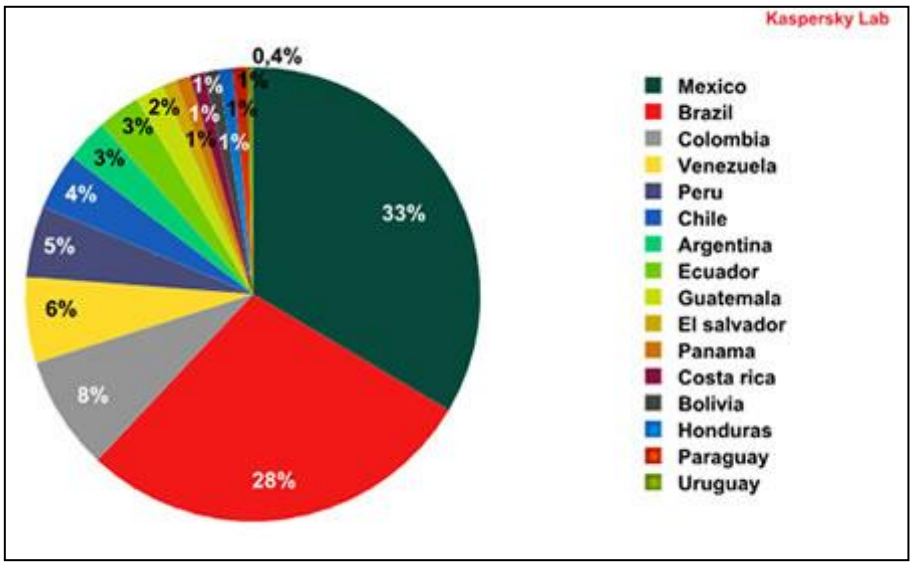
Según el sitio web segu-info.com.ar, en su sección de reportes estadísticos "Casi el 70% de las Pymes de la región sufrieron ciberataques El 68,6 por ciento de las pequeñas y medianas empresas (Pymes) de 12 países de Latinoamérica sufrieron ataques de virus informáticos en los últimos 12 meses, según un estudio realizado por la firma Prince & Cooke para Microsoft.

Durante 2009, esa cifra ascendía a 73% y, de esa cifra, 35% habían tenido éxito En estos casos, todas las empresas resultaron afectadas por pérdidas de tiempo por inactividad debido al robo de información….." (tomado de https://seguinfo.wordpress.com/2010/11/18/casi-el-70-de-las-pymes-de-la-region-sufriero n-ciberataques/)

Nuestro país, no se encuentra libre de estos ataques, ya que según datos estadísticos de la compañía Karpersky Labs., creadora del software de prevención y protección de ataques, más completos y reconocidos en el Ecuador, indica como lo muestra el gráfico,

que ocupamos el 8vo. puesto en comparación con otros países latinoamericanos, en relación con el número de habitantes.

"Ecuador, que ocupa el octavo lugar a pesar de ser uno de los países más pequeños de América Latina, debe su posición a que la banca ecuatoriana aún no tiene mecanismos de seguridad eficientes para combatir el crimen cibernético moderno y el sistema legislativo del país no está preparado para luchar de forma eficiente contra el cibercrimen. Además, los criminales se aprovechan de que la economía es dolarizada y por esto las ganancias a través de robo de dinero vienen de una divisa fuerte." (http://identidadesenpeligro.wordpress.com/2011/02/07/ataques-informaticos-en-america-latina-en-el-2010/)



Prevenir todo este sistema de posibles ataques a través de Internet, hace necesario, cambiar la visión sobre la importancia de la Seguridad de la Información que tienen los usuarios y propietarios de negocios y empresas, al destacar y considerar aspectos como rubros de inversión de capital en la implementación de Políticas de Seguridad a fin de proteger la confidencialidad, integridad y disponibilidad de la información, e incluso considerar una reorganización administrativa de las funciones y responsabilidades del departamento de sistemas, en el caso de existir.

Es por todo esto, que el desarrollo de la presente monografía es de suma importancia ya que promueve y fomenta el desarrollo de una cultura de seguridad en nuestro país al plantear un modelo de Seguridad Informática que analiza políticas, procedimientos y herramientas de software libre para garantizar la integridad de la información dentro de una red local con acceso a Internet.

1.3 OBJETIVOS.

1.3.1. Objetivo general.

Crear un modelo de implementación de Políticas de seguridad basadas en la ISO 27001 y en las herramientas de software libre necesarias para la administración de la Seguridad Informática de una red local.

1.3.2. Objetivos específicos.

- Identificar riesgos y vulnerabilidades.
- Desarrollar políticas de seguridad de la información en base a los requerimientos del negocio.
- Analizar las ventajas y desventajas de algunas herramientas de seguridad de software libre.
- Diseñar un plan de implementación de software de seguridad.
- Realizar pruebas de seguridad.

CAPITULO II

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Una vez que hemos revisado algunos conceptos básicos sobre seguridad de la información y la necesidad de implementar mecanismos de prevención a través de una serie de herramientas de tipo software y/o hardware, así como políticas de seguridad informática, vamos a revisar algunos conceptos básicos para su implementación.

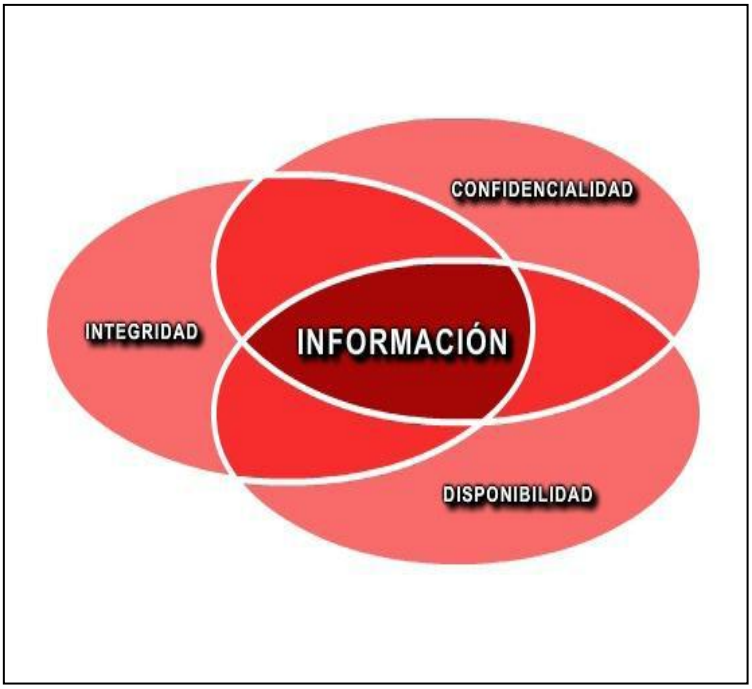
2.1. POLÍTICAS DE SEGURIDAD INFORMÁTICA.

Una Política de Seguridad Informática (PSI), es una herramienta organizacional que tiene por finalidad concienciar a los colaboradores de una empresa o negocio sobre la importancia y sensibilidad de la información, involucra directamente a los responsables de la seguridad del área informática; conocida como departamento de sistemas quienes sientan las bases de lo que está o no permitido hacer.

Se define como un documento que refleja una declaración de intención de los dueños de una empresa o negocio de establecer normas (directrices) para el uso de los sistemas de información existentes. Es decir; recopila y define una serie de normas, reglamentos y protocolos a seguir; medidas para proteger la seguridad de los sistemas.

Es importante señalar que, toda política de seguridad, debe tomar como uno de sus puntos más elementales, la comunicación con el o los usuarios, para que sea concebida no como un mero reglamento de sanciones, sino como una herramienta de trabajo que describa que se desea proteger, cómo y la razón de ello. Es por esto, que las políticas de seguridad deben redactarse en un lenguaje sencillo y entendible, libre de tecnicismos y términos ambiguos que impidan una comprensión clara de las mismas, claro está sin sacrificar su precisión.

Una política de la seguridad de la información debe reflejar los elementos claves de seguridad como: velar por la integridad, disponibilidad, privacidad de la información, además de su control, autenticidad y utilidad.



Cuadro tomado de http://jmpovedar.files.wordpress.com/2011/03/mc3b3dulo-4.pdf

Son elementos claves de una política de seguridad de la información:

- "Ser holística (cubrir todos los aspectos relacionados con la misma). No tiene sentido proteger el acceso con una puerta blindada si a esta no se la ha cerrado con llave.
- Adecuarse a las necesidades y recursos. No tiene sentido adquirir una caja fuerte para proteger un lápiz.
- Ser atemporal. El tiempo en el que se aplica no debe influir en su eficacia y eficiencia.
- Definir estrategias y criterios generales a adoptar en distintas funciones y actividades, donde se conocen las alternativas ante circunstancias repetidas."

(Tomado de: http://www.segu-info.com.ar/politicas/riesgos.htm)

Sin embargo, pese a la importancia de la implementación de una política de seguridad informática, su puesta en funcionamiento no es tan fácil; requiere el compromiso de los altos ejecutivos, su integración en las estrategias de la empresa o negocio, a su misión y visión. Deben, también, seguir un proceso de actualización periódica sujeta a los cambios organizacionales relevantes, como son: el aumento de personal, cambios en la infraestructura computacional, alta rotación de personal, desarrollo de nuevos servicios, regionalización de la empresa, cambio o diversificación del área de negocios, etc.

Finalmente, es importante señalar que las políticas por sí solas no son una garantía para la seguridad de la empresa, ellas deben responder a intereses y necesidades empresariales basadas en la visión de negocio, que lleven a un esfuerzo conjunto de sus actores.

2.2. EVALUACIÓN DE RIESGO.

La evaluación de riesgo hace referencia a la evaluación de las amenazas y vulnerabilidades relativas a la información, instalaciones de procesamiento, probabilidad de ocurrencia y el potencial impacto en la empresa o negocio.

El término amenaza hace referencia a una acción o acciones que pueden ocasionar consecuencias negativas en una empresa, pueden ser de carácter físico o lógico. Mientras que el término vulnerabilidad, se refiere a una debilidad que puede ser explotada con la materialización de una o varias amenazas a un activo.

El sitio web http://www.arcert.gov.ar/politica/ nos presenta un listado de las principales amenazas a considerar, con una descripción de cada uno:

- Ingeniería Social
- Phishing
- Escaneo de Puertos
- Wardialers
- Código Malicioso / Virus
- Exploits
- Ataques de Contraseña
- Control Remoto de Equipos
- Eavesdropping
- Man-in-the-Middle
- Defacement
- IP Spoofing - MAC Address Spoofing
- Robo de identidad
- Repetición de Transacción
- Backdoors
- DHCP Starvation
- Trashing
- Denegación de Servicio
- Denegación de Servicio Distribuida
- Fraude Informático
- Software Ilegal
- Acceso a Información Confidencial Impresa
- Daños Físicos al Equipamiento
- Robo de Equipamiento
- Pérdida de Copias de Resguardo

Y la descripción de cada una de ellas:

Ingeniería Social

Consiste en utilizar artilugios, tretas y otras técnicas para el engaño de las personas logrando que revelen información de interés para el atacante, como ser contraseñas de acceso. Se diferencia del resto de las amenazas básicamente porque no se aprovecha de debilidades y vulnerabilidades propias de un componente informático para la obtención de información.

Phishing

Consiste en el envío masivo de mensajes electrónicos que fingen ser notificaciones oficiales de entidades/empresas legítimas con el fin de obtener datos personales y bancarios de los usuarios.

Escaneo de Puertos

Consiste en detectar qué servicios posee activos un equipo, con el objeto de ser utilizados para los fines del atacante.

Wardialers

Se trata de herramientas de software que utilizan el acceso telefónico de una máquina para encontrar puntos de conexión telefónicos en otros equipos o redes, con el objeto de lograr acceso o recabar información.

Código Malicioso / Virus

Se define como todo programa o fragmento del mismo que genera algún tipo de problema en el sistema en el cual se ejecuta, interfiriendo de esta forma con el normal funcionamiento del mismo. Existen diferentes tipos de código malicioso; a continuación mencionamos algunos de ellos:

- **Bombas lógicas**
  Se encuentran diseñados para activarse ante la ocurrencia de un evento definido en su lógica.
- **Troyanos**
  Suele propagarse como parte de programas de uso común y se activan cuando los mismos se ejecutan.
- **Gusanos**
  Tienen el poder de autoduplicarse causando efectos diversos.
- **Cookies**
  Son archivos de texto con información acerca de la navegación efectuada por el usuario en Internet e información confidencial del mismo que pueden ser obtenidos por atacantes.
- **Keyloggers**
  Es una aplicación destinada a registrar todas las teclas que un usuario tipea en su computadora; algunos de ellos además registran otro tipo de información útil para un atacante, como ser, imágenes de pantalla.
- **Spyware**
  Aplicaciones que recogen y envían información sobre las páginas web que más frecuentemente visita un usuario, tiempo de conexión, datos relativos al equipo en el que se encuentran instalados (sistema operativo, tipo de procesador, memoria, etc.) e, incluso, hay algunos diseñados para informar

de si el software que utiliza el equipo es original o no.

Exploits

Se trata de programas o técnicas que explotan una vulnerabilidad de un sistema para el logro de los objetivos del atacante, como ser, intrusión, robo de información, denegación de servicio, etc.

Ataques de Contraseña

Consiste en la prueba metódica de contraseñas para lograr el acceso a un sistema, siempre y cuando la cuenta no presente un control de intentos fallidos de logueo.
Este tipo de ataques puede ser efectuado:
o Por diccionario: existiendo un diccionario de palabras, una herramienta intentará acceder al sistema probando una a una las palabras incluidas en el diccionario.
o Por fuerza bruta: una herramienta generará combinaciones de letras números y símbolos formando posibles contraseñas y probando una a una en el login del sistema.

Control Remoto de Equipos

Un atacante puede tomar el control de un equipo en forma remota y no autorizada, mediante la utilización de programas desarrollados para tal fin, e instalados por el atacante mediante, por ejemplo la utilización de troyanos.

Eavesdropping

El eavesdropping es un proceso por el cual un atacante capta de información (cifrada o no) que no le iba dirigida. Existen diferentes tipos de técnicas que pueden utilizarse:

- **Sniffing**
  Consiste en capturar paquetes de información que circulan por la red con la utilización de una herramienta para dicho fin, instalada en un equipo conectado a la red; o bien mediante un dispositivo especial conectado al cable. En redes inalámbricas la captura de paquetes es más simple, pues no requiere de acceso físico al medio.
  Relacionados con este tipo de ataque, pueden distinguirse también las siguientes técnicas:
  - **AIRsniffing**: consiste en capturar paquetes de información que circulan por redes inalámbricas. Para ello es necesario contar con una placa de red "wireless" configurada en modo promiscuo y una antena.
  - **War Driving** y **Netstumbling**: estas técnicas se valen del AIRsniffing, ya

que consisten en circular (generalmente en un vehículo) por un vecindario o zona urbana, con el objeto de capturar información transmitida a través de redes inalámbricas. Esto es posible debido a que generalmente las ondas de transmisión de información en redes inalámbricas se expanden fuera del área donde se ubican los usuarios legítimos de la red, pudiendo ser alcanzadas por atacantes. Lo que en ocasiones las hace más vulnerables es la falta de seguridad con que se encuentran implementadas.

- **Desbordamiento de CAM**.
  Se trata de inundar la tabla de direcciones de un switch con el objeto de bloquear la capacidad que éste posee de direccionar cada paquete exclusivamente a su destino. De esta forma el atacante podrá efectuar sniffing de los paquetes enviados por un switch, cuando en condiciones normales un switch no es vulnerable a este tipo de ataques.
- **VLAN hopping**
  Las VLANs son redes LAN virtuales las cuales se implementan para generar un control de tráfico entre las mismas, de forma que los equipos conectados a una VLAN no posean acceso a otras. Este tipo de ataque pretende engañar a un switch (sobre el cual se implementan VLANs) mediante técnicas de Switch Spoofing logrando conocer los paquetes de información que circulan entre VLANs.
- **STP manipulation**
  Este tipo de ataque es utilizado en topologías que cuentan con un árbol de switches que implementan el protocolo Spanning Tree Protocol para coordinar su comunicación. El equipo atacante buscará convertirse en la "raíz" de dicho árbol, con el objeto de poder tener acceso a los paquetes de información que circulan por todos los switches.

Man-in-the-middle

El atacante se interpone entre el origen y el destino en una comunicación pudiendo conocer y/o modificar el contenido de los paquetes de información, sin esto ser advertido por las víctimas. Esto puede ocurrir en diversos ambientes, como por ejemplo, en comunicaciones por e-mail, navegación en Internet, dentro de una red LAN, etc..

Defacement

Consiste en la modificación del contenido de un sitio web por parte de un atacante.

IP Spoofing - MAC Address Spoofing

El atacante modifica la dirección IP o la dirección MAC de origen de los paquetes de información que envía a la red, falsificando su identificación para hacerse pasar por otro usuario. De esta manera, el atacante puede asumir la identificación de un

usuario válido de la red, obteniendo sus privilegios.

Repetición de Transacción

Consiste en capturar la información correspondiente a una transacción efectuada en la red interna o en Internet, con el objeto de reproducirla posteriormente. Esto cobra real criticidad en transacciones monetarias.

Backdoors

También denominados “puertas traseras”, consisten en accesos no convencionales a los sistemas, los cuales pueden permitir efectuar acciones que no son permitidas por vías normales. Generalmente son instalados por el atacante para lograr un permanente acceso al sistema.

DHCP Starvation

El atacante busca reemplazar al servidor DHCP que se encuentra funcionando en la red, de forma de asignar a los clientes direcciones IP y otra información (como ser el servidor Gateway) de acuerdo a su conveniencia. De esta forma podría luego simular ser el Gateway e interceptar la información que los clientes envíen, con el tipo de ataque Man-in-the-middle.

Trashing

Consiste en la búsqueda de información dentro de la basura. Esto puede representar una amenaza importante para usuarios que no destruyen la información crítica o confidencial al eliminarla.

Denegación de Servicio

Su objetivo es degradar considerablemente o detener el funcionamiento de un servicio ofrecido por un sistema o dispositivo de red. Existen diferentes técnicas para la explotación de este tipo de ataques:

- Envío de paquetes de información mal conformados de manera de que la aplicación que debe interpretarlo no puede hacerlo y colapsa.
- Inundación de la red con paquetes (como ser ICMP - ping, TCP – SYN, IP origen igual a IP destino, etc.) que no permiten que circulen los paquetes de información de usuarios.
- Bloqueo de cuentas por excesivos intentos de login fallidos.
- Impedimento de logueo del administrador.

Denegación de Servicio Distribuida

Su objetivo es el mismo que el perseguido por un ataque de denegación de servicio común, pero en este caso se utilizan múltiples equipos para generar el ataque.

Fraude Informático

Se trata del perjuicio económico efectuado a una persona mediante la utilización de un sistema informático, ya sea, modificando datos, introduciendo datos falsos o verdaderos o cualquier elemento extraño que sortee la seguridad del sistema.

Software Ilegal

Consiste en la instalación de software licenciado sin contar con la licencia correspondiente que habilita su uso, o mediante la falsificación de la misma.

Acceso a Información Confidencial Impresa

Ocurre cuando información confidencial impresa es obtenida por personal no autorizado debido a que la misma no es resguardada adecuadamente mediante por ejemplo, una política de limpieza de escritorios.

Daños Físicos al Equipamiento

Los daños físicos pueden ser ocasionados por:

- Acciones intencionadas
- Negligencia de los usuarios (ej.: derrame de líquidos, golpes, etc.)
- Catástrofes naturales (ej.: fallas eléctricas, incendio, inundación, falta de refrigeración, etc.)

Robo de Equipamiento o Componentes

El robo puede involucrar todo un equipo o de parte del mismo, ej.: un disco rígido. Puede ocurrir por un deficiente control de acceso establecido al centro de cómputos (o recinto donde residen los equipos: servidores, routers, switches, etc.), así como a las propias instalaciones del Organismo.

- Pérdida de Copias de Resguardo

  Si no existen adecuadas medidas de seguridad física para las copias de resguardo, las mismas pueden dañarse, por ejemplo, en caso de ser afectadas por desastres como un incendio, inundación, o incluso por robo. Asimismo, una administración inadecuada de los medios físicos de almacenamiento puede provocar la obsolescencia de los mismos (ej.: reutilización excesiva de cintas). Por otra parte, se debe tener en cuenta la obsolescencia tecnológica de los medios de almacenamiento con el paso del tiempo, de manera de actualizarlos adecuadamente para permitir su restauración en caso de ser necesaria.

- Robo de identidad

  Ocurre cuando alguien obtiene y utiliza, mediante medios informáticos, información personal ajena (nombre, número de tarjeta de crédito, información bancaria, número de afiliado a un sistema de salud, etc.) sin su autorización, con el propósito de realizar actividades fraudulentas.

La evaluación de riesgo, es el punto de partida para la elaboración de la política de seguridad informática de una empresa o negocio. Su análisis inicia con el cálculo de las posibilidades que existen de que ocurra un suceso negativo, para luego continuar con la evaluación económica del impacto de ese suceso, sus probabilidades de ocurrencia versus el costo. Continuando con el inventario de los activos físicos que se desean proteger versus las amenazas existentes.

A continuación se realizará el levantamiento de activos o inventario de activos que recopila los principales activos de información de la empresa o negocio, entendiéndose como activo de información todo elemento que contiene o manipula información como por ejemplo: ficheros y bases de datos, contratos y acuerdo, documentación del sistema, manuales de los usuarios, aplicaciones, software del sistema, equipos informáticos, equipo de comunicaciones, servicios informáticos y de comunicaciones, utilidades generales como calefacción, iluminación, energía y aire acondicionado y las personas quienes generan, transmiten y destruyen información.

Cuadro tomado de http://jmpovedar.files.wordpress.com/2011/03/mc3b3dulo-7.pdf-15-05-2011

El inventario de activos para la implementación de la gestión de seguridad no debe duplicar los activos, pero sí, destaca los más importantes, ya que incluye toda la información para mantenerlos operativos e incluso poder recuperarlos en case de desastre.

Cuadro tomado de http://jmpovedar.files.wordpress.com/2011/03/mc3b3dulo-7.pdf-15-05-2011

LEVANTAMIENTO DE ACTIVOS DEL CYBERCAFÉ 10 DE AGOSTO

CÓDIGO	TIPO DE ACTIVO	CANTIDAD	DESCRIPCIÓN	PROPIETARIO	LOCALIZACIÓN
1	EQUIPOS	1	SERVIDOR PRINCIPAL	DUEÑO	ENTRADA DEL LOCAL COMERCIAL
2		5	TERMINALES COMPUTADOR DE ESCRITORIO	DUEÑO	EN EL MEZANINE
3	COMUNICACION	2	BASES CELULARES	DUEÑO	SOBRE LA INFRAESTRUCTURA DE LAS CABINAS
4		1	MODEM	DUEÑO	DETRÁS DE LA FOTOCOPIADORA
5		1	RUTEADOR	DUEÑO	DETRÁS DE LA FOTOCOPIADORA
6		5	TELÉFONOS		CABINAS
7	EQ. AUXILIAR	1	FOTOCOPIADORA/IMPRESOR		AL LADO DEL SERVIDOR
8		1	ESCANNER		SOBRE EL SERVIDOR
9		1	FAX		DETRÁS DE LA FOTOCOPIADORA
10	APLICACIONES	1	BONUS COMUNICACIONES PROGRAMA PARA EL MANEJO DE LLAMADAS CELULARES.		SERVIDOR
11		1	CONTROLCYBER PROGRAMA PARA DAR ACCESO A INTERNET		SERVIDOR
12		5	LICENCIAS WINDOWS XP		SERVIDOR
12		1	AXESS SITIO WEB PARA RECARGAS		SERVIDOR

			ELECTRÓNICAS		
13	SERVICIOS	1	PLAN CORPORATIVO PARA ACCESO A INTERNET BANDA ANCHA		CABLEADO DESDE LA CALLE HASTA EL SERVIDOR
14	DATOS	1	SALDO DE DINERO PARA REALIZAR RECARGAS		SERVIDOR
15		1	ARCHIVO EXCEL CON CUADRE DE CAJA DIARIO		SERVIDOR
16	PERSONAL	1	DUEÑO DEL NEGOCIO		SERVIDOR
17		1	EMPLEADO		SERVIDOR
18		50	CLIENTES DIARIOS		CABINAS, TERMINALES

Una vez identificados los activos es necesario establecer parámetros para evaluar la disponibilidad, integridad y confidencialidad de cada activo siguiendo los siguientes criterios:

Disponibilidad: Hace referencia a la importancia o el problema que ocasionaría que el activo no estuviera disponible. Podemos considerar una escala de 0 a 3 se podría valorar como sigue:

VALOR	CRITERIO
0	No aplica / No es relevante
1	Debe estar disponible al menos el 10% del tiempo
2	Debe estar disponible al menos el 50% del tiempo
3	Debe estar disponible al menos el 99% del tiempo

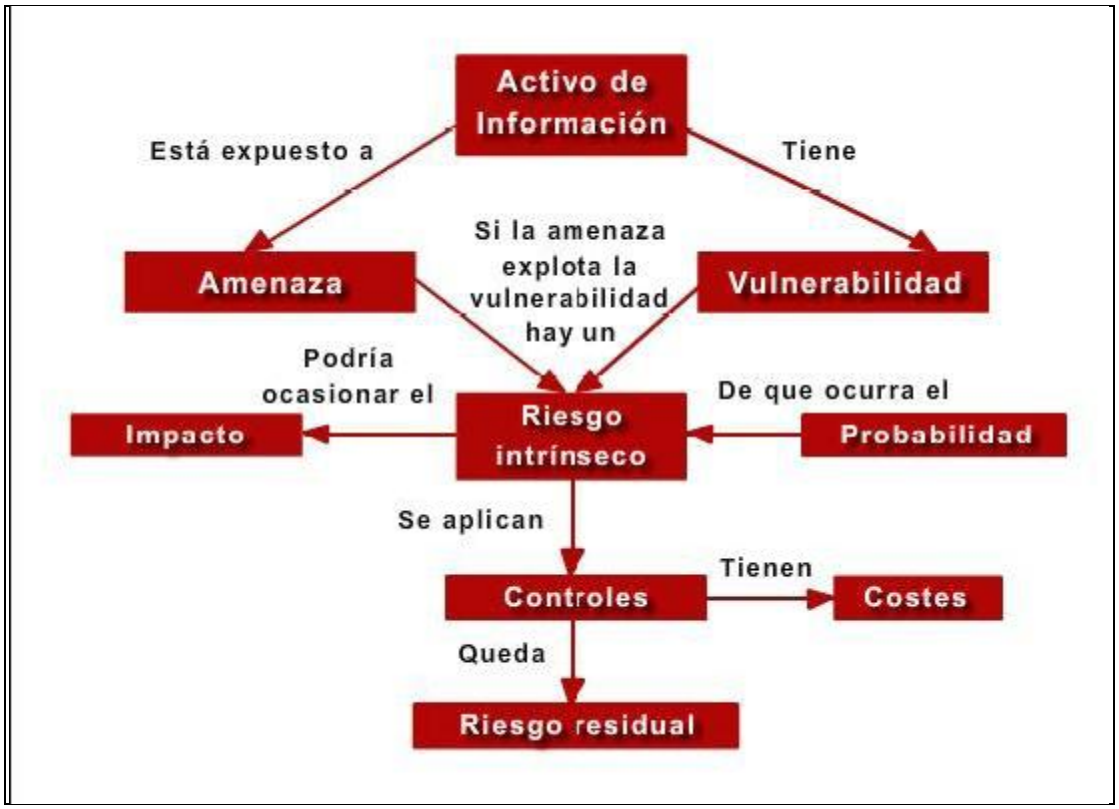
Integridad: Hace referencia a la importancia que tendría si el activo fuera alterado sin autorización ni control. Una posible escala es:

VALOR	CRITERIO
0	No aplica / No es relevante
1	No es relevante los errores que tenga o la información que falte
2	Tiene que estar correcto y completo al menos en un 50%
3	Tiene que estar correcto y completo al menos en un 95%

Confidencialidad: Hace referencia a la importancia que tendría que al activo se accediera de manera no autorizada. La escala en este caso podría ser:

VALOR	CRITERIO
0	No aplica / No es relevante
1	Daños muy bajos, el incidente no trascendería del área afectada
2	Serían relevantes, el incidente implicaría a otras áreas
3	Los daños serían catastróficos, la reputación y la imagen de la organización se verían comprometidas

Una vez establecidos estos parámetros puede establecer el análisis de riesgos a través de diferentes metodologías:



Cuadro tomado de http://jmpovedar.files.wordpress.com/2011/03/mc3b3dulo-7.pdf-15-05-2011

Las metodologías disponibles para el análisis de riesgos, según el sitio web http://jmpovedar.files.wordpress.com/2011/03/mc3b3dulo-7.pdf-15-05-2011 son:

Análisis holandés A&K.

Es método de análisis de riesgos, del que hay publicado un manual, que ha sido desarrollado por el Ministerio de Asuntos Internos de Holanda, y se usa en el gobierno y a menudo en empresas holandesas.

CRAMM.

Es un método de análisis de riesgos desarrollado por el gobierno británico y cuenta con una herramienta, ya que es un método difícil de usar sin ella. Está basado en las mejores prácticas de la administración pública británica, por lo que es más adecuado para organizaciones grandes, tanto públicas como privadas.

EBIOS.

Es un juego de guías mas una herramienta de código libre gratuita, enfocada a gestores del riesgo de TI. Desarrollada en un principio por el gobierno francés, ha tenido una gran difusión y se usa tanto en el sector público como en el privado no sólo de Francia sino en otros países. La metodología EBIOS consta de un ciclo de cinco fases:

- *Fase 1*. Análisis del contexto, estudiando cuales son las dependencias de los procesos del negocio respecto a los sistemas de información.
- *Fases 2 y 3*, Análisis de las necesidades de seguridad y de las amenazas, determinando los puntos de conflicto.
- *Fases 4 y 5*, Resolución del conflicto, estableciendo los objetivos de seguridad necesarios y suficientes, con pruebas de su cumplimiento y dejando claros cuales son los riesgos residuales.

IT-GRUNDSCHUTZ (Manual de protección básica de TI)

Desarrollado en Alemania por la Oficina Federal de la Seguridad de la Información (BSI en sus siglas alemanas). Este manual proporciona un método para establecer un SGSI en cualquier organización, con recomendaciones técnicas para su implantación. El proceso de seguridad de TI propuesto por esta metodología sigue los siguientes pasos:

- Iniciar el proceso.
- Definir los objetivos de seguridad y el contexto de la organización.
- Establecer la organización para la seguridad de TI.
- Proporcionar recursos.

- Crear el concepto de la seguridad de TI.
- Análisis de la estructura de TI.
- Evaluación de los requisitos de protección.
- Modelado.
- Comprobación de la seguridad de TI.
- Planificación e implantación.
- Mantenimiento, seguimiento y mejora del proceso.

La metodología incluye listas de amenazas y controles de seguridad que se pueden ajustar a las necesidades de cada organización.

MAGERIT.

Desarrollado por el Ministerio de Administraciones Públicas español, es una metodología de análisis de riesgos que describe los pasos para realizar un análisis del estado de riesgo y para gestionar su mitigación, detalla las tareas para llevarlo a cabo de manera que el proceso esté bajo control en todo momento y contempla aspectos prácticos para la realización de de un análisis y una gestión realmente efectivos. Cuenta con detallados catálogos de amenazas, vulnerabilidades y salvaguardas. Cuenta con una herramienta, denominada PILAR para el análisis y la gestión de los riesgos de los sistemas de información que tiene dos versiones, una completa para grandes organizaciones y otra simplificada para las pequeñas.

Manual de Seguridad de TI Austriaco.

Consta de dos partes, en la primera se describe el proceso de la gestión de la seguridad de TI, incluyendo el análisis de riesgos y la segunda es un compendio de 230 medidas de seguridad. Es conforme con la Norma ISO/IEC IS 13335 y en parte con la ISO 27002.

MARION – MEHARI.

El primigenio MARION (Método de Análisis de Riesgos por Niveles), basado en una metodología de auditoría, permitía estimar el nivel de riesgos de TI de una organización. Sustituido por MEHARI, este método de análisis de riesgo cuenta con un modelo de evaluación de riesgos y módulos de componentes y procesos. Con MEHARI se detectan vulnerabilidades mediante auditorías y se analizan situaciones de riesgo.

Métodos ISF para la evaluación y gestión de riesgos.

El Information Security Forum. (ISF) es una importante asociación internacional. Su Estándar de Buenas Prácticas es un conjunto de principios y objetivos para la seguridad de la información con buenas prácticas asociadas a los mismos. El Estándar cubre la gestión de la seguridad a nivel corporativo, las aplicaciones críticas del negocio, las instalaciones de los sistemas de información, las redes y el desarrollo de sistemas. El Estándar contiene:

- FIRM, una metodología para el seguimiento y control del riesgo. o Una herramienta para la gestión del riesgo. o SARA, otra metodología para analizar el riesgo en sistemas críticos. o SPRINT, una metodología para hacer análisis de impacto en el negocio y analizar el riesgo en sistemas importantes pero no críticos.
- SARA, otra metodología para analizar el riesgo en sistemas críticos.
- Una herramienta para la gestión del riesgo.
- SPRINT, una metodología para hacer análisis de impacto en el negocio y analizar el riesgo en sistemas importantes pero no críticos.

Norma ISO/IEC IS 27005.

La Norma habla de la gestión de los riesgos de la seguridad de la información de manera genérica, utilizando para ello el modelo PDCA, y en sus anexos se pueden encontrar enfoques para la realización de análisis de riesgos, así como un catálogo de amenazas, vulnerabilidades y técnicas para valorarlos.

OCTAVE.

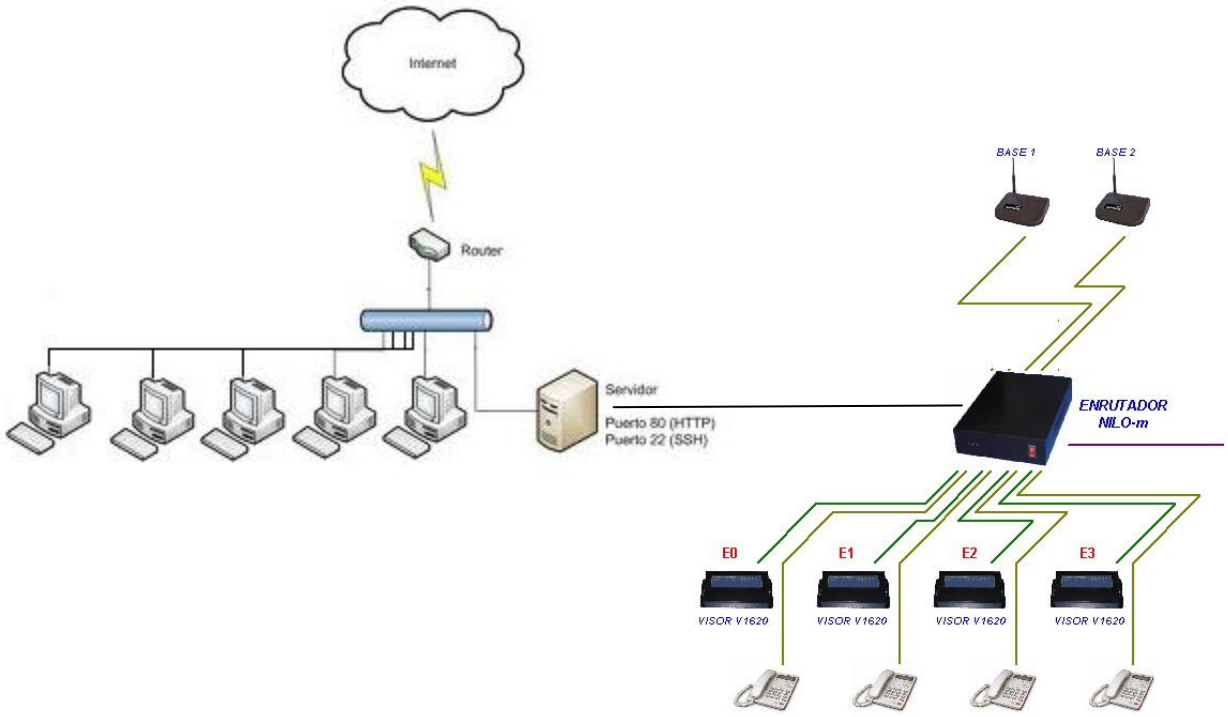
(Operationally Critical Threat, Asset, and Vulnerability EvaluationSM (OCTAVE®), desarrollado en EEUU por el SEI, en un una metodología para recoger y analizar información de manera que se pueda diseñar una estrategia de protección y planes de mitigación de riesgo basados en los riesgos operacionales de seguridad de la organización. Hay dos versiones, una para grandes organizaciones y otra para pequeñas, de menos de 100 empleados.

SP800-30 NIST Risk Management Guide for Information Technology Systems.

Desarrollado por el NIST estadounidense, es una guía detallada de las consideraciones que deben hacerse para llevar a cabo una evaluación y una gestión de riesgos orientada a la seguridad de los sistemas de información.

El análisis de riesgo para este proyecto sigue los lineamientos de la norma MAGERIT, descrita a continuación:

1.- Esquema del negocio.



Al momento de realizar el levantamiento del esquema, es importante anotar que 2 estaciones de trabajo estaban fuera de servicio en reparación.

2.- Procesos realizados en el negocio.

CÓDIGO	DESCRIPCION
P1	Llamadas telefónicas celulares.
P2	Navegación Internet.
P3	Recargas electrónicas.
P4	Impresión y/o fotocopiado.
P5	Facturación.
P6	Cobro
P7	Servicio de software de oficina para realizar trabajos (xls, doc, ppt).
P8	Servicio de envío de fax.

ACTIVOS DE INFORMACIÓN DEL CIBERCAFÉ 10 DE AGOSTO

HARDWARE

COD.	TIPO DE ACTIVO	DESCRIPCIÓN	PROCESO	SERIE	DIRECCIÓN IP	CONF.	DISPO.	INTEG.
1	EQUIPOS	SERVIDOR	P2	# N/A	190.168.0.1	3	3	100%
1	EQUIPOS	SERVIDOR	P3	# N/A	190.168.0.1	3	2	100%
1	EQUIPOS	SERVIDOR	P4	# N/A	190.168.0.1	2	2	100%
1	EQUIPOS	SERVIDOR	P5	# N/A	190.168.0.1	3	2	100%
1	EQUIPOS	SERVIDOR	P6	# N/A	190.168.0.1	3	3	100%
1	EQUIPOS	SERVIDOR	P7	# N/A	190.168.0.1	3	2	100%
2	EQUIPOS	ESTACIONES DE TRABAJO 1	P2	# N/A	190.168.0.110	1	1	1
2	EQUIPOS	ESTACIONES DE TRABAJO 1	P4	# N/A	190.168.0.110	1	2	2
2	EQUIPOS	ESTACIONES DE TRABAJO 1	P7	# N/A	190.168.0.110	1	2	2
3	EQUIPOS	ESTACIONES DE TRABAJO 2	P2	# N/A	190.168.0.120	1	2	2
3	EQUIPOS	ESTACIONES DE TRABAJO 2	P4	# N/A	190.168.0.120	1	2	2
3	EQUIPOS	ESTACIONES DE TRABAJO 2	P7	# N/A	190.168.0.120	1	2	2
4	EQUIPOS	ESTACIONES DE TRABAJO 3	P2	# N/A	190.168.0.150	1	2	2
4	EQUIPOS	ESTACIONES DE TRABAJO 3	P4	# N/A	190.168.0.150	1	2	2

4	EQUIPOS	ESTACIONES DE TRABAJO 3	P7	# N/A	190.168.0.150	1	2	2
5	EQUIPO	ALARMA PARADOX SECURITY SYSTEM	P1,2,3,4,5,6,7,8	No se ve, pegado a la pared	N/A	3	2	1

ACTIVOS DE INFORMACIÓN DEL CIBERCAFÉ 10 DE AGOSTO

SOFTWARE

COD.	TIPO DE ACTIVO	DESCRIPCIÓN	PROCESO	PROV.	LICENCIA ORIGINAL		# ACTIVACIÓN	FECHA COMPRA (DD/MM/AA)	VENCTO. LICENCIA	DIRECCIÓN IP	CONF.	DISPO.	INTEG.
					SI EXISTE	NO EXISTE							
1	SOFTWARE	WINDOWS XP	P2	N/A		X	N/A	N/A	N/A	190.168.0.1	1	3	100%
1	SOFTWARE	WINDOWS XP	P3	N/A		X				190.168.0.1	3	3	100%
1	SOFTWARE	WINDOWS XP	P4	N/A		X				190.168.0.1	1	2	100%
1	SOFTWARE	WINDOWS XP	P5	N/A		X				190.168.0.1	3	1	100%
1	SOFTWARE	WINDOWS XP	P6	N/A		X				190.168.0.1	3	3	100%
1	SOFTWARE	WINDOWS XP	P7	N/A		X				190.168.0.1	1	1	100%
2	SOFTWARE	WINDOWS XP-2	P2	N/A		X	N/A	N/A	N/A	190.168.0.110	1	2	100%
2	SOFTWARE	WINDOWS XP-2	P4	N/A		X				190.168.0.110	1	2	100%
2	SOFTWARE	WINDOWS XP-2	P7	N/A		X				190.168.0.110	1	2	100%
3	SOFTWARE	WINDOWS XP-3	P2	N/A		X	N/A	N/A	N/A	190.168.0.120	1	2	100%
3	SOFTWARE	WINDOWS XP-3	P4	N/A		X				190.168.0.120	1	2	100%
3	SOFTWARE	WINDOWS XP-3	P7	N/A		X				190.168.0.120	1	2	100%
4	SOFTWARE	WINDOWS XP-4	P2	N/A		X	N/A	N/A	N/A	190.168.0.150	1	2	100%
4	SOFTWARE	WINDOWS XP-4	P4	N/A		X				190.168.0.150	1	2	100%
4	SOFTWARE	WINDOWS XP-4	P7	N/A		X				190.168.0.150	1	2	100%
5	SOFTWARE	BONUS COMUNICACIONES para llamadas celulares	P1	N/A			N/A	N/A	N/A	190.168.0.1	3	2	3
5	SOFTWARE	BONUS COMUNICACIO	P5	N/A			N/A	N/A	N/A	190.168.0.1	3	3	100%

		NES para llamadas celulares											
5	SOFTWARE	BONUS COMUNICACIONES para llamadas celulares	P6	N/A			N/A	N/A	N/A	190.168.0.1	3	2	100%
6	SOFTWARE	CONTROLCYBER para acceso a Internet, tiempo y costo	P2	Internet	X		N/A	N/A	N/A	190.168.0.1	3	2	100%
6	SOFTWARE	CONTROLCYBER para acceso a Internet, tiempo y costo	P4	Internet	X		N/A	N/A	N/A	190.168.0.1	1	2	2
6	SOFTWARE	CONTROLCYBER para acceso a Internet, tiempo y costo	P7	Internet	X		N/A	N/A	N/A	190.168.0.1	2	2	2
7	SOFTWARE	MICROSOFT OFFICE 2007	P7	N/A		X	N/A	N/A	N/A	190.168.0.110	1	3	2
8	SOFTWARE	NOD 32	P2	Internet	X		N/A	N/A	N/A				
8	SOFTWARE	NOD 32	P7	Internet	X		N/A	N/A	N/A				
9	SOFTWARE	KASPERSKY INTERNET SECURITY 7.0	P2	N/A		X	N/A	11/06/2010	11/06/2011	190.168.0.1	3	3	100%
9	SOFTWARE	KASPERSKY INTERNET SECURITY 7.0	P3	N/A		X	N/A	11/06/2010	11/06/2011	190.168.0.1	3	3	100%

9	SOFTWARE	KASPERSKY INTERNET SECURITY 7.0	P7	N/A		X	N/A	11/06/2010	11/06/2011	190.168.0.1	3	3	100%

ACTIVOS DE INFORMACIÓN DEL CIBERCAFÉ 10 DE AGOSTO

EQUIPO DE COMUNICACIÓN

COD.	TIPO DE ACTIVO	DESCRIPCIÓN	PROCESO	SERIE	DIRECCIÓN IP	CONF.	DISPO.	INTEG.
1	COMUNICACIÓN	BASE CELULAR FWT	P1	# 354779034072679	N/A	3	2	2
2	COMUNICACIÓN	BASE CELULAR FWT	P1	# 355689010930064	N/A	3	2	2
3	COMUNICACIÓN	MODEM MOTOROLA	P2	# C. D6VD43RGG578	N/A	3	3	3
3	COMUNICACIÓN	MODEM MOTOROLA	P3	# C. D6VD43RGG578	N/A	3	2	2
3	COMUNICACIÓN	MODEM MOTOROLA	P5	# C. D6VD43RGG578	N/A	3	2	100%
3	COMUNICACIÓN	MODEM MOTOROLA	P6	# C. D6VD43RGG578	N/A	3	2	100%
4	COMUNICACIÓN	RUTEADOR ADVANTEK NETWORKS	P2	# N/A	N/A	2	2	2
4	COMUNICACIÓN	RUTEADOR ADVANTEK NETWORKS	P4	# N/A	N/A	2	2	2
4	COMUNICACIÓN	RUTEADOR ADVANTEK NETWORKS	P7	# N/A	N/A	1	2	2
5	COMUNICACIÓN	ADAPTADOR	P1	# FLI00G204697	192.168.0.50	1	2	2

		TELEFONICO DE ITERNET LINKSYS						
6	COMUNICACIÓN	TELÉFONO PANASONIC	P1	# 5EAAC252779	N/A	1	2	2
7	COMUNICACIÓN	TELÉFONO PANASONIC	P1	# 5EAAC259339	N/A	1	2	2
8	COMUNICACIÓN	TELÉFONO PANASONIC	P1	# 3LAAB042971	N/A	1	2	2
9	COMUNICACIÓN	TELÉFONO PANASONIC	P1	# 6FAAC503510	N/A	1	2	2
10	COMUNICACIÓN	TELÉFONO PANASONIC	P8	# 5EAAC259420	N/A	1	2	2

ACTIVOS DE INFORMACIÓN DEL CIBERCAFÉ 10 DE AGOSTO

EQUIPO DE AUXILIAR

COD.	TIPO DE ACTIVO	DESCRIPCIÓN	PROCESO	SERIE	DIRECCIÓN IP	CONF.	DISPO.	INTEG.
1	EQUIPO AUXILIAR	FOTOCOPIADORA /IMPRESORA RICOH 1035	P4	# H7926700787	192.168.0.10	2	2	3
2	EQUIPO AUXILIAR	IMPRESORA MULTIFUNCIÓN EPSON ST. TX110	P7	# LJUZ242114	N/A	2	2	2
3	EQUIPO AUXILIAR	FAX PANASONIC MOD. #KX-FT931L9	P8	# 7EBWA142678	N/A	2	2	2
4	EQUIPO AUXILIAR	IMPRESORA EPSON	P1	# CQXG053403	N/A	1	2	100%

ACTIVOS DE INFORMACIÓN DEL CIBERCAFÉ 10 DE AGOSTO

EDIFICIO

COD.	TIPO DE ACTIVO	DIRECCIÓN	TELÉFONO	PROCESO	CONF.	DISPO.	INTEG.
1	EDIFICIO	AV. 10 DE AGOSTO 2-06	4096949	P1	1	3	2
1	EDIFICIO	AV. 10 DE AGOSTO 2-06	4096949	P2	1	3	2
1	EDIFICIO	AV. 10 DE AGOSTO 2-06	4096949	P4	1	3	2
1	EDIFICIO	AV. 10 DE AGOSTO 2-06	4096949	P7	1	3	2
1	EDIFICIO	AV. 10 DE AGOSTO 2-06	4096949	P8	1	3	2

ACTIVOS DE INFORMACIÓN DEL CIBERCAFÉ 10 DE AGOSTO

PERSONAL

COD.	TIPO DE ACTIVO	NOMBRES	CARGO	PROCESO	TELÉFONO	CÉDULA	DIRECCIÓN I	CONF.	DISPO.	INTEG.
1	PERSONAL	PABLO ROJAS	PROPIETARIO	P1	09565xxxx	0102015XXXX	Av. 10 de agosto 2-06	1	2	3
1	PERSONAL	PABLO ROJAS	PROPIETARIO	P2	09565xxxx	0102015XXXX	Av. 10 de agosto 2-06	1	2	3
1	PERSONAL	PABLO ROJAS	PROPIETARIO	P3	09565xxxx	0102015XXXX	Av. 10 de agosto 2-06	1	2	3
1	PERSONAL	PABLO ROJAS	PROPIETARIO	P4	09565xxxx	0102015XXXX	Av. 10 de agosto 2-06	1	2	3
1	PERSONAL	PABLO ROJAS	PROPIETARIO	P5	09565xxxx	0102015XXXX	Av. 10 de agosto 2-06	1	2	3
1	PERSONAL	PABLO ROJAS	PROPIETARIO	P6	09565xxxx	0102015XXXX	Av. 10 de agosto 2-06	1	2	3
1	PERSONAL	PABLO ROJAS	PROPIETARIO	P7	09565xxxx	0102015XXXX	Av. 10 de agosto 2-06	1	2	3
1	PERSONAL	PABLO ROJAS	PROPIETARIO	P8	09565xxxx	0102015XXXX	Av. 10 de agosto 2-06	1	2	3
2	PERSONAL	PAULINA ROJAS	AYUDANTE	P1	08415xxxx	0154240XXXX	Av. 10 de agosto 2-06	1	2	3
2	PERSONAL	PAULINA ROJAS	AYUDANTE	P2	08415xxxx	0154240XXXX	Av. 10 de agosto 2-06	1	2	3
2	PERSONAL	PAULINA ROJAS	AYUDANTE	P3	08415xxxx	0154240XXXX	Av. 10 de agosto 2-06	1	2	3

2	PERSONAL	PAULINA ROJAS	AYUDANTE	P4	08415xxxx	0154240XXXX	Av. 10 de agosto 2-06	1	2	3
2	PERSONAL	PAULINA ROJAS	AYUDANTE	P5	08415xxxx	0154240XXXX	Av. 10 de agosto 2-06	1	2	3
2	PERSONAL	PAULINA ROJAS	AYUDANTE	P6	08415xxxx	0154240XXXX	Av. 10 de agosto 2-06	1	2	3
2	PERSONAL	PAULINA ROJAS	AYUDANTE	P7	08415xxxx	0154240XXXX	Av. 10 de agosto 2-06	1	2	3
2	PERSONAL	PAULINA ROJAS	AYUDANTE	P8	08415xxxx	0154240XXXX	Av. 10 de agosto 2-06	1	2	3

ACTIVOS DE INFORMACIÓN DEL CIBERCAFÉ 10 DE AGOSTO

INFORMACIÓN ELECTRÓNICA

COD.	TIPO DE ACTIVO	DESCRIPCIÓN	PROCESO	UBICACIÓN	CONF.	DISPO.	INTEG.
1	INF. ELECTRÓNICA	RECARGAS	P3	SERVIDOR	3	3	100%
1	INF. ELECTRÓNICA	RECARGAS	P5	SERVIDOR	1	2	100%
1	INF. ELECTRÓNICA	RECARGAS	P6	SERVIDOR	1	3	100%
2	INF. ELECTRÓNICA	DATOS DE CAJA	P6	SERVIDOR	3	1	100%
3	INF. ELECTRÓNICA	SALDO DE LLAMADAS POR INTERNET	P1	SERVIDOR	3	2	100%

ACTIVOS DE INFORMACIÓN DEL CIBERCAFÉ 10 DE AGOSTO

INFORMACIÓN EN PAPEL

COD.	TIPO DE ACTIVO	DESCRIPCIÓN	PROCESO	UBICACIÓN	CONF.	DISPO.	INTEG.
1	INF. EN PAPEL	FACTURA DE COMPRA	P6	ARCHIVO		2	100%
2	INF. EN PAPEL	FACTURA DE VENTA	P5	ARCHIVO	1	2	100%

ACTIVOS DE INFORMACIÓN DEL CIBERCAFÉ 10 DE AGOSTO

CONTRATOS POR SERVICIOS

COD.	TIPO DE ACTIVO	NUM. CONTRATO	DESCRIPCIÓN	PROCESO	NOMBRE PROVEEDOR	FECHA INICIO CONTRATO (DD/MM/AA)	FECHA VENC. CONTRATO (DD/MM/AA)	CONF.	DISPO.	INTEG.
1	SERVICIOS	4863565	PLAN DE INTERNET CORPORATIVO	P2	TV-CABLE	27/08/2010	27/08/2011	2	3	100%
1	SERVICIOS	4863565	PLAN DE INTERNET CORPORATIVO	P3	TV-CABLE	27/08/2010	27/08/2011	2	2	100%
2	SERVICIOS	0111100	RECARGADE BASES CELULARES PARA LLAMADAS	P1	ALEGRO	27/08/2010	27/08/2011	2	2	2
3	SERVICIOS	N/A	RECARGAS ELECTRONICAS VIA WEB	P3	XY-PREPAGO	10/03/2011	N/A	3	2	100%
4	SERVICIOS	N/A	RECARGA ELECTRÓNICA PARA LLAMADAS INTERNACIONALES.	P1	CAFÉ FONE	N/A	N/A	3	2	100%
5	SERVICIOS	N/A	LÍNEA TELEFÓNICA COMERCIAL	P8	ETAPA	N/A	N/A	1	1	2

6	SERVICIOS	N/A	ENERGÍA ELECTRICA	P 1-8	EMPRESA ELÉCTRICA CENTRO SUR	N/A	N/A	3	3	100%

Luego de haber identificado y clasificado los activos del Cibercafé 10 de agosto, se procedió a armar el cuadro general que muestra los activos de información con cada uno de sus componentes:

CUADRO GENERAL

ACTIVO	HARD.	SOFT	COM.	AUX.	INF.ELE	PERS.	EDIF.	SERV	INF.PAP.
AI01	1	1	3	1	1	1	1	1	2
	5	5	4	2	2	2		2	
		6	5	4	3			3	
		7						4	
		9						6	
VALOR	3	3	3	3	3	3	3	3	2
AI02	2	2	3	1		1	1	1	
	3	3	4	2		2		6	
	4	4							
	5	6							
		7							
		8							
VALOR	2	3	3	3		3	3	3	
AI03	1	5	1	4	3	1	1	2	2
	5		2-3-4			2		4	
			5					1	
			6					5	

	7				6
	8				
	9				
VALOR T	3		3	3	2
AI04	10	1	1	1	5
		3	2		6
VALOR T	2	3	3	3	3

Esta tabla nos permite determinar cuáles son los valores más altos para cada uno de los activos de información y así poder establecer que soluciones se van a establecer a corto (nivel 3), mediano (nivel 2) y largo plazo (nivel 1). De igual forma la implementación de las políticas de seguridad de la información para mitigar los riegos se implementarán siguiendo esta escala.

A continuación se muestra una tabla de riesgos y su posible factor; es decir la probabilidad de que ocurra serían:

RIESGO	FACTOR
Robo de hardware	Alto
Robo de información	Bajo
Vandalismo	Medio
Fallas de equipos	Alto
Equivocaciones	Bajo
Accesos no autorizados	Bajo
Fraude	Bajo
Fuego	Medio
Temblor-Terremoto	Muy Bajo
Inundación	Bajo
Demanda BCA	Alto

2.3. ESTRATEGIAS DE SEGURIDAD.

Una estrategia de seguridad de la información hace referencia a los pasos a seguir para proteger y abarcar todos los niveles de seguridad tratados en los temas anteriores. Estas estrategias están plasmadas en las políticas de seguridad a través de la implementación de un plan de seguridad.

Las estrategias de seguridad, pueden ser de dos tipos:

Estrategia Proactiva: También conocida como de previsión de ataques, es decir, proteger y proceder, define el conjunto de pasos a seguir para reducir significativamente las vulnerabilidades existentes. Para desarrollar esta estrategia es necesario conocer el daño que ocasiona un ataque, las debilidades y puntos vulnerables explotados.

Estrategia Reactiva: O estrategia posterior, es decir, perseguir y procesar, define los pasos a seguir para evaluar el daño causado por un ataque, repararlo e implementar un plan de contingencia.

Las estrategias de seguridad, también definen algunos lineamientos relacionados con los recursos compartidos como: lo que no está permitido está prohibido y lo que NO se prohíbe expresamente está permitido, que de manera general se constituyen en la base de toda política de seguridad regulando procedimientos y su implementación.

ESTRATEGIAS

ACTIVO	RIEGO	VALOR	POLÍTICA	ESTRATEGIA	TAREA
AI01	**Robo de hardware**	Alto	Debe protegerse los equipos para disminuir el riesgo de robo, destrucción y mal uso	Implementar medidas de seguridad	Contratar servicio de vigilancia privada. Contratar y activar servicio de botón de auxilio.
			La pérdida o robo de cualquier componente de hardware o programa de software debe ser reportada inmediatamente.	Manual de procedimientos.	Llevar un registro.
			Los equipos deben marcarse para su identificación y control de inventario. Los registros de inventario deben mantenerse actualizados	Inventario.	Registro y codificación de activos
			No pueden moverse los equipos o reubicarlos sin permiso. Para llevar un equipo fuera del cibercafé se	Manual de procedimientos.	Registro de activos enviados a reubicados.

		requiere una autorización escrita del propietario.		
Robo de información	Bajo	No divulgar información confidencial del negocio a personas no autorizadas.	Contrato de confidencialidad	Reunión con un abogado.
		No permitir y no facilitar el uso de los sistemas informáticos del negocio a personas no autorizadas.	Control de acceso	Listado de usuarios.
		Proteger meticulosamente su contraseña y evitar que sea vista por otros en forma inadvertida.	Contraseñas seguras	Reubicación de servidor.
		Seleccionar una contraseña robusta que no tenga relación obvia con el usuario, sus familiares, el grupo de trabajo, y otras asociaciones parecidas.	Contraseñas seguras	Definir contraseña
		Reportar inmediatamente a su jefe inmediato cualquier evento que pueda comprometer la seguridad de la Institución y sus recursos	Manual de procedimientos	Socializar normas.

	informáticos, como por ejemplo contagio de virus, intrusos, modificación o pérdida de datos y otras actividades poco usuales.		
	Los datos confidenciales que aparezcan en la pantalla deben protegerse de ser vistos por otras personas mediante disposición apropiada del mobiliario de la oficina y protector de pantalla. Cuando ya no se necesiten o no sean de utilidad, los datos confidenciales se deben borrar.		Reubicación de monitor. Implementar protector de pantalla
	A menos que se indique lo contrario, los usuarios deben asumir que todo el software del Cibercafé está protegido por derechos de autor y requiere licencia de uso. Por tal razón es ilegal y está terminantemente prohibido hacer copias o usar ese software para fines personales	Control de licencias o propiedad intelectual.	Carteles de aviso

		La información del cibercafé clasificada como confidencial o de uso restringido, debe guardarse de forma segura	Respaldo de información.	Definir un lugar dentro del negocio. Sacar una copia.
		Siempre que sea posible, debe eliminarse información confidencial de los computadores y unidades de disco duro antes de que les mande a reparar. Si esto no es posible, se debe asegurar que la reparación sea efectuada por empresas responsables, con las cuales se haya firmado un contrato de confidencialidad	Contrato de confidencialidad	Lista de proveedores.
Vandalismo	Medio	Se debe contratar un seguro de robo o incendio para mitigar el daño de actos vandálicos y recuperar el negocio en el menor tiempo posible.	Contrato con Aseguradora.	Buscar compañías y bróker aseguradores. Seleccionar y contratar la compañía de seguros.
Fallas de equipos	Alto	Debe respetarse y no modificar la configuración de hardware y software.	Control de accesos por usuario	Creación de usuarios con privilegios.
		No se permite fumar, comer o beber	Manual de procedimientos	Carteles de aviso.

	mientras se está usando el servidor.		Señalización
	Deben protegerse los equipos de riesgos del medioambiente (por ejemplo, polvo, incendio y agua).	Proteger contra riesgos del medio ambiente.	Limpieza periódica de polvo. Adquisición de cobertores.
	Deben usarse reguladores de energía eléctrica en cada uno de los terminales y en los servidores deben usarse UPS	Instalación y uso de Reguladores de energía eléctrica	Adquirir reguladores. Adquirir UPS
	Cualquier falla en los computadores o en la red debe reportarse inmediatamente ya que podría causar problemas serios como pérdida de la información o indisponibilidad de los servicios	Manual de procedimientos	Carteles de aviso.
	Debe instalarse y activarse una herramienta antivirus, la cual debe mantenerse actualizada. Si se detecta la presencia de un virus u otro agente potencialmente peligroso, se debe notificar inmediatamente al	Instalación y uso de antivirus	Buscar herramientas gratuitas o no muy costosas. Analizar costos y aplicabilidad.

	Administrador de Sistemas (en este caso el propietario) y poner la PC en cuarentena hasta que el problema sea resuelto		
	Debe utilizarse un programa antivirus para examinar todo software que venga de afuera o descargue	Instalación y uso de antivirus	Buscar herramientas gratuitas o no muy costosas. Analizar costos y aplicabilidad.
	No debe utilizarse software bajado de Internet en el servidor y en general software que provenga de una fuente no confiable, a menos que se haya sido comprobado en forma rigurosa y que esté aprobado su uso por el propietario.	Instalación de herramientas Anti-Spy, Firewall.	Restringir el acceso, bloqueando sitios web.
	No deben usarse USB u otros medios de almacenamiento en cualquier computadora del cibercafé sin que antes hayan sido verificados que estén libres de virus u otros agentes	Instalación y uso de antivirus	Buscar herramientas gratuitas o no muy costosas. Analizar costos y aplicabilidad.

		dañinos		
Equivocaciones	Bajo	Todos los cambios en las bases celulares, en los servidores y equipos de red del Cibercafé, incluyendo la instalación de nuevo software, el cambio de direcciones IP, la reconfiguración de ruteadores y switchs, deben ser documentados y debidamente aprobados, excepto si se trata de una situación de emergencia. Todo esto es para evitar problemas por cambios apresurados y que puedan causar interrupción de las comunicaciones, caída de la red, denegación de servicio o acceso inadvertido a información confidencial	Manual de procedimientos	Documentación de cambios y procedimientos.
		Cuando un empleado recibe una nueva cuenta, debe firmar un documento donde declara conocer las políticas y procedimientos de	Contrato de confidencialidad	Redactar lineamientos legales con un abogado.

	seguridad, y acepta sus responsabilidades con relación al uso de esa cuenta		
	La navegación en Internet en el servidor para fines personales no debe hacerse a expensas del tiempo y recursos del negocio. En tal sentido, no deberán usarse las instalaciones y recursos del cibercafé para fines ajenos a lo laboral	Manual de procedimientos	Documentación de cambios y procedimientos.
	Se prohíbe el uso de aplicaciones y/o herramientas no permitidas que saturen los canales de comunicación del cibercafé, tales como gestores de descarga de archivos multimedia (audio y/o videos), Ares, Torrent entre otros	Control de accesos por usuario	Creación de usuarios con privilegios.
	Se restringe el uso de aplicativos de comunicación tipo chat (Facebook, Messenger, Skype y similares), su instalación deberá ser autorizada por	Control de accesos por usuario	Creación de usuarios con privilegios.

		el propietario		
Accesos no autorizados	Bajo	No permitir y no facilitar el uso de los sistemas informáticos del negocio a personas no autorizadas.	Manual de procedimientos	Documentación de cambios y procedimientos.
		La solicitud de una nueva cuenta o el cambio de privilegios debe ser hecha por escrito y debe ser debidamente aprobada	Manual de procedimientos	Documentación de cambios y procedimientos.
		No debe concederse una cuenta a personas que no sean empleados del Cibercafé a menos que estén debidamente autorizados, en cuyo caso la cuenta debe expirar automáticamente al cabo de un lapso de 30 días	Manual de procedimientos	Documentación de cambios y procedimientos.
		Privilegios especiales, tal como la posibilidad de modificar o borrar los archivos de otros usuarios, sólo deben otorgarse a aquellos directamente responsable de la administración o de la seguridad de	Manual de procedimientos	Documentación de cambios y procedimientos.

	los sistemas		
	No deben otorgarse cuentas a técnicos de mantenimiento ni permitir su acceso remoto a menos que el Administrador de Sistemas determine que es necesario. En todo caso esta facilidad sólo debe habilitarse para el periodo de tiempo requerido para efectuar el trabajo (como por ejemplo, el mantenimiento remoto, daño del servidor)	Manual de procedimientos	Documentación de cambios y procedimientos.
	Se prohíbe el uso de cuentas anónimas o de invitado (guest) y los usuarios deben entrar al sistema mediante cuentas que indiquen claramente su identidad	Manual de procedimientos	Documentación de cambios y procedimientos.
	Toda cuenta queda automáticamente suspendida después de un cierto periodo de inactividad. El periodo recomendado es de 30 días	Manual de procedimientos	Documentación de cambios y procedimientos.

	Cuando un usuario (empleado) renuncia, es despedido o se finiquita su contrato con el Cibercafé, debe desactivarse su cuenta antes de que deje el cargo	Manual de procedimientos	Documentación de cambios y procedimientos.
	El usuario no debe guardar su contraseña en una forma legible en archivos en disco, y tampoco debe escribirla en papel y dejarla en sitios donde pueda ser encontrada. Si hay razón para creer que una contraseña ha sido comprometida, debe cambiarla inmediatamente. No deben usarse contraseñas que son idénticas o substancialmente similares a contraseñas previamente empleadas. Siempre que sea posible, debe impedirse que los usuarios vuelvan a usar contraseñas anteriores	Contraseña segura.	Definir contraseña.
	Nunca debe compartirse la contraseña o revelarla a otros. El	Manual de procedimientos	Documentación de cambios y

	hacerlo expone al usuario a las consecuencias por las acciones que los otros hagan con esa contraseña		procedimientos.
	Está prohibido el uso de contraseñas de grupo para facilitar el acceso a archivos, aplicaciones, bases de datos, computadoras, redes, y otros recursos del sistema. Esto se aplica en particular a la contraseña del administrador	Manual de procedimientos	Documentación de cambios y procedimientos.
	La contraseña inicial emitida a un nuevo usuario sólo debe ser válida para la primera sesión. En ese momento, el usuario debe escoger otra contraseña	Manual de procedimientos	Documentación de cambios y procedimientos.
	Las contraseñas predefinidas que traen los equipos nuevos tales como ruteadores, switchs, etc., deben cambiarse inmediatamente al ponerse en servicio el equipo	Manual de procedimientos	Documentación de cambios y procedimientos.
	Para prevenir ataques, cuando el	Manual de procedimientos	Documentación de

	software del sistema lo permita, debe limitarse a 3 el número de consecutivos de intentos infructuosos de introducir la contraseña, luego de lo cual la cuenta involucrada queda suspendida y se alerta al Administrador del sistema. Si se trata de acceso remoto vía módem por discado, la sesión debe ser inmediatamente desconectada		cambios y procedimientos.
	Si no ha habido ninguna actividad en un terminal, PC o estación de trabajo durante un cierto periodo de tiempo, el sistema debe automáticamente borrar la pantalla y suspender la sesión. El periodo recomendado de tiempo es de 15 minutos. El re-establecimiento de la sesión requiere que el usuario proporcione se autentique mediante su contraseña (o utilice otro mecanismo, por ejemplo,	Implementar medidas de seguridad	Configurar protector de pantallas con contraseña.

	tarjeta inteligente o de proximidad)		
	Si el sistema de control de acceso no está funcionando propiamente, debe rechazar el acceso de los usuarios hasta que el problema se haya solucionado	Implementar medidas de seguridad	Reiniciar el programa.
	Los archivos de bitácora (logs) y los registros de auditoría (audit trails) que graban los eventos relevantes sobre la seguridad de los sistemas informáticos y las comunicaciones, deben revisarse periódicamente y guardarse durante un tiempo prudencial de por lo menos tres meses. Dicho archivos son importantes para la detección de intrusos, brechas en la seguridad, investigaciones, y otras actividades de auditoría. Por tal razón deben protegerse para que nadie los pueda alterar y que sólo los pueden leer las	Manual de procedimientos	Documentación de cambios y procedimientos.

		personas autorizadas		
		Los servidores de red y los equipos de comunicación (bases celulares, ruteadores, etc.) deben estar ubicados en locales apropiados, protegidos contra daños y robo. Debe restringirse severamente el acceso a estos locales y a los cuartos de cableado a personas no autorizadas mediante el uso de cerraduras y otros sistemas de acceso	Reingeniería del negocio.	Reubicación del servidor. Nuevo servidor. Señalización. Cerradura.
	Fraude	Bajo	No utilizar los recursos informáticos (hardware, software o datos) y de telecomunicaciones (teléfono, fax) para otras actividades que no estén directamente relacionadas con el área del negocio.	Manual de procedimientos	Documentación de cambios y procedimientos.
	Fuego	Medio	Periódicamente debe hacerse el respaldo de los datos guardados en el servidor y las copias de respaldo deben guardarse en un lugar seguro,	Respaldo de información	Comprar disco de respaldo. Establecer frecuencia de respaldo y ubicación de

		a prueba de hurto, incendio e inundaciones. Los programas y datos vitales para la operación del Cibercafé debe guardarse en otra sede, lejos del negocio		respaldo.
	Temblor-Terremoto	Muy Bajo	Periódicamente debe hacerse el respaldo de los datos guardados en el servidor y las copias de respaldo deben guardarse en un lugar seguro, a prueba de hurto, incendio e inundaciones. Los programas y datos vitales para la operación del Cibercafé debe guardarse en otra sede, lejos del negocio	Respaldo de información	Comprar disco de respaldo. Establecer frecuencia de respaldo y ubicación de respaldo.
	Inundación	Bajo	Periódicamente debe hacerse el respaldo de los datos guardados en el servidor y las copias de respaldo deben guardarse en un lugar seguro, a prueba de hurto, incendio e inundaciones. Los programas y datos vitales para la operación del	Respaldo de información	Comprar disco de respaldo. Establecer frecuencia de respaldo y ubicación de respaldo.

		Cibercafé debe guardarse en otra sede, lejos del negocio		
Demanda	Alto	No debe utilizarse software bajado de Internet en el servidor y en general software que provenga de una fuente no confiable, a menos que se haya sido comprobado en forma rigurosa y que esté aprobado su uso por Informática.	Licenciamiento de Software	Buscar cotizaciones. Analizar presupuesto inversión. Buscar y analizar otras opciones.
		Para ayudar a restaurar los programas originales no dañados o infectados, deben hacerse copias de todo software nuevo antes de su uso, y deben guardarse tales copias en un lugar seguro	Respaldo de información	Comprar disco de respaldo. Establecer frecuencia de respaldo y ubicación de respaldo.
		Los recursos, servicios y conectividad disponibles vía Internet abren nuevas oportunidades, pero también introducen nuevos riesgos. En particular, no debe enviarse a través de Internet mensajes con	Manual de procedimientos	Uso de Outlook, Outlook Express

			información confidencial a menos que estén cifrada. Para tal fin debe utilizarse PGP (Pretty Good Privacy), Outlook, Outlook Express u otros productos previamente aprobados por Informática		
			Es política del Cibercafé no monitorear regularmente las comunicaciones. Sin embargo, el uso y el contenido de las comunicaciones puede ocasionalmente ser supervisado en caso de ser necesario para actividades de mantenimiento, seguridad o auditoría. Puede ocurrir que el personal técnico vea el contenido de un mensaje de un empleado individual durante el curso de resolución de un problema	Manual de procedimientos	Documentación de cambios y procedimientos. Carteles de aviso.
AI02	**Robo de hardware**	Medio	Debe protegerse los equipos para disminuir el riesgo de robo, destrucción y mal uso	Implementar medidas de seguridad	Contratar servicio de vigilancia privada. Contratar y activar

				servicio de botón de auxilio.
		Los equipos deben marcarse para su identificación y control de inventario. Los registros de inventario deben mantenerse actualizados	Inventario.	Registro y codificación de activos
		No pueden moverse los equipos o reubicarlos sin permiso. Para llevar un equipo fuera del cibercafé se requiere una autorización escrita del propietario.	Manual de procedimientos.	Registro de activos enviados a reubicados. Carteles de aviso.
Vandalismo	Medio	Se debe contratar un seguro de robo o incendio para mitigar el daño de actos vandálicos y recuperar el negocio en el menor tiempo posible.	Contrato con Aseguradora.	Buscar compañías y bróker aseguradores. Seleccionar y contratar la compañía de seguros.
Fallas de equipos	Alto	Deben protegerse los equipos de riesgos del medioambiente (por ejemplo, polvo, incendio y agua).	Proteger contra riesgos del medio ambiente.	Limpieza periódica de polvo.Adquisición de cobertores.
		Debe respetarse y no modificar la	Control de accesos por	Lista de clientes.

	configuración de hardware y software.	usuario	
	No se permite fumar, comer o beber mientras se está usando una estación de trabajo.	Manual de procedimientos	Carteles de aviso. Señalización.
	Deben usarse reguladores de energía eléctrica en cada uno de los terminales y en los servidores deben usarse UPS	Instalación y uso de Reguladores de energía eléctrica	Adquirir reguladores. Adquirir UPS
	Cualquier falla en los computadores o en la red debe reportarse inmediatamente ya que podría causar problemas serios como pérdida de la información o indisponibilidad de los servicios	Manual de procedimientos	Carteles de aviso.
	Debe instalarse y activarse una herramienta antivirus, la cual debe mantenerse actualizada. Si se detecta la presencia de un virus u otro agente potencialmente peligroso, se debe notificar inmediatamente al	Instalación y uso de antivirus	Buscar herramientas gratuitas o no muy costosas. Analizar costos y aplicabilidad.

	Administrador de Sistemas (en este caso el propietario) y poner la PC en cuarentena hasta que el problema sea resuelto		
	Debe utilizarse un programa antivirus para examinar todo software que venga de afuera o descargue	Instalación y uso de antivirus	Buscar herramientas gratuitas o no muy costosas. Analizar costos y aplicabilidad.
	No debe utilizarse software bajado de Internet en el servidor y en general software que provenga de una fuente no confiable, a menos que se haya sido comprobado en forma rigurosa y que esté aprobado su uso por Informática.	Instalación de herramientas Anti-Spy, Firewall.	Restringir el acceso, bloqueando sitios web.
	No deben usarse USB u otros medios de almacenamiento en cualquier computadora del cibercafé sin que antes hayan sido verificados que estén libres de virus u otros agentes	Instalación y uso de antivirus	Buscar herramientas gratuitas o no muy costosas. Analizar costos y aplicabilidad.

		dañinos		
Accesos no autorizados	Bajo	Los usuarios no deben intentar violar los sistemas de seguridad y de control de acceso. Acciones de esta naturaleza se consideran violatorias de las políticas del Cibercafé, pudiendo ser causal de resolución de contrato o negación del servicio ofrecido	Control de accesos por usuario	Creación de usuarios con privilegios.
		Para tener evidencias en casos de acciones disciplinarias y judiciales, cierta clase de información debe capturarse, grabarse y guardarse cuando se sospeche que se esté llevando a cabo abuso, fraude u otro crimen que involucre los sistemas informáticos	Implementar medidas de seguridad	Contratar servicio de vigilancia privada. Contratar y activar servicio de botón de auxilio.
Fraude	Bajo	Tomando en cuenta que cierta información está dirigida a personas específicas y puede no ser apta para otros, dentro y fuera del Cibercafé,	Manual de procedimientos	Carteles de aviso. Señalización

		se debe ejercer cierta cautela al remitir los mensajes. En todo caso no debe remitirse información confidencial del Cibercafé sin la debida aprobación		
	Fuego	Medio	Periódicamente debe hacerse el respaldo de los datos guardados en el servidor y las copias de respaldo deben guardarse en un lugar seguro, a prueba de hurto, incendio e inundaciones. Los programas y datos vitales para la operación del Cibercafé debe guardarse en otra sede, lejos del negocio	Respaldo de información	Comprar disco de respaldo. Establecer frecuencia de respaldo y ubicación de respaldo.
	Temblor-Terremoto	Muy Bajo	Periódicamente debe hacerse el respaldo de los datos guardados en el servidor y las copias de respaldo deben guardarse en un lugar seguro, a prueba de hurto, incendio e inundaciones. Los programas y datos vitales para la operación del	Respaldo de información	Comprar disco de respaldo. Establecer frecuencia de respaldo y ubicación de respaldo.

		Cibercafé debe guardarse en otra sede, lejos del negocio		
Inundación	Bajo	Periódicamente debe hacerse el respaldo de los datos guardados en el servidor y las copias de respaldo deben guardarse en un lugar seguro, a prueba de hurto, incendio e inundaciones. Los programas y datos vitales para la operación del Cibercafé debe guardarse en otra sede, lejos del negocio	Respaldo de información	Comprar disco de respaldo. Establecer frecuencia de respaldo y ubicación de respaldo.
Demanda	Alto	No debe utilizarse software bajado de Internet en el servidor y en general software que provenga de una fuente no confiable, a menos que se haya sido comprobado en forma rigurosa y que esté aprobado su uso por Informática.	Licenciamiento de Software	Buscar cotizaciones. Analizar presupuesto inversión. Buscar y analizar otras opciones.
		Los recursos, servicios y conectividad disponibles vía Internet abren nuevas oportunidades, pero	Manual de procedimientos	Uso de Outlook, Outlook Express

	también introducen nuevos riesgos. En particular, no debe enviarse a través de Internet mensajes con información confidencial a menos que estén cifrada. Para tal fin debe utilizarse PGP (Pretty Good Privacy), Outlook, Outlook Express u otros productos previamente aprobados por Informática		
	Es política del Cibercafé no monitorear regularmente las comunicaciones. Sin embargo, el uso y el contenido de las comunicaciones puede ocasionalmente ser supervisado en caso de ser necesario para actividades de mantenimiento, seguridad o auditoría. Puede ocurrir que el personal técnico vea el contenido de un mensaje de un empleado individual durante el curso de resolución de un problema	Manual de procedimientos	Documentación de cambios y procedimientos. Carteles de aviso.

AI03	**Robo de hardware**	Alto	Debe protegerse los equipos para disminuir el riesgo de robo, destrucción y mal uso	Implementar medidas de seguridad	Contratar servicio de vigilancia privada. Contratar y activar servicio de botón de auxilio.
			Los equipos deben marcarse para su identificación y control de inventario. Los registros de inventario deben mantenerse actualizados	Inventario.	Registro y codificación de activos
			No pueden moverse los equipos o reubicarlos sin permiso. Para llevar un equipo fuera del cibercafé se requiere una autorización escrita del propietario.	Manual de procedimientos.	Registro de activos enviados a reubicados.
	Robo de información	Bajo	Debe instalarse y activarse una herramienta antivirus, la cual debe mantenerse actualizada. Si se detecta la presencia de un virus u otro agente potencialmente peligroso, se debe notificar inmediatamente al	Instalación y uso de antivirus	Buscar herramientas gratuitas o no muy costosas. Analizar costos y aplicabilidad.

		Administrador de Sistemas (en este caso el propietario) y poner la PC en cuarentena hasta que el problema sea resuelto		
		Debe utilizarse un programa antivirus para examinar todo software que venga de afuera o descargue	Instalación y uso de antivirus	Buscar herramientas gratuitas o no muy costosas. Analizar costos y aplicabilidad.
Vandalismo	Medio	Se debe contratar un seguro de robo o incendio para mitigar el daño de actos vandálicos y recuperar el negocio en el menor tiempo posible.	Contrato con Aseguradora.	Buscar compañías y bróker aseguradores. Seleccionar y contratar la compañía de seguros.
Fallas de equipos	Alto	Deben usarse reguladores de energía eléctrica en cada uno de los terminales y en los servidores deben usarse UPS	Instalación y uso de Reguladores de energía eléctrica	Adquirir reguladores. Adquirir UPS
		No debe utilizarse software bajado de Internet en el servidor y en general software que provenga de una fuente no confiable, a menos que	Instalación de herramientas Anti-Spy, Firewall.	Restringir el acceso, bloqueando sitios web.

		se haya sido comprobado en forma rigurosa y que esté aprobado su uso por Informática.		
	Fuego	Medio	Periódicamente debe hacerse el respaldo de los datos guardados en el servidor y las copias de respaldo deben guardarse en un lugar seguro, a prueba de hurto, incendio e inundaciones. Los programas y datos vitales para la operación del Cibercafé debe guardarse en otra sede, lejos del negocio	Respaldo de información	Comprar disco de respaldo. Establecer frecuencia de respaldo y ubicación de respaldo.
	Temblor-Terremoto	Muy Bajo	Periódicamente debe hacerse el respaldo de los datos guardados en el servidor y las copias de respaldo deben guardarse en un lugar seguro, a prueba de hurto, incendio e inundaciones. Los programas y datos vitales para la operación del Cibercafé debe guardarse en otra sede, lejos del negocio	Respaldo de información	Comprar disco de respaldo. Establecer frecuencia de respaldo y ubicación de respaldo.

Fraude	Bajo	Los sistemas de comunicación del cibercafé generalmente sólo deben usarse para actividades de trabajo. El uso personal en forma ocasional es permisible siempre y cuando consuma una cantidad mínima de tiempo y recursos, y además no interfiera con la productividad del negocio	Manual de procedimientos	Documentación de cambios y procedimientos. Carteles de aviso.
		Se prohíbe el uso de los sistemas de comunicación para actividades comerciales privadas	Manual de procedimientos	Documentación de cambios y procedimientos. Carteles de aviso.
		De manera consistente con prácticas generalmente aceptadas, el propietario del negocio procesa datos estadísticos sobre el uso de los sistemas de comunicación. Como ejemplo, los reportes de la central telefónica, celulares contienen detalles sobre el número llamado, la	Manual de procedimientos	Documentación de cambios y procedimientos. Carteles de aviso.

			duración de la llamada, y la hora en que se efectuó la llamada		
AI04	**Robo**		Debe protegerse los equipos para disminuir el riesgo de robo, destrucción y mal uso	Implementar medidas de seguridad	Contratar servicio de vigilancia privada. Contratar y activar servicio de botón de auxilio.
			Los equipos deben marcarse para su identificación y control de inventario. Los registros de inventario deben mantenerse actualizados	Inventario.	Registro y codificación de activos
			No pueden moverse los equipos o reubicarlos sin permiso. Para llevar un equipo fuera del cibercafé se requiere una autorización escrita del propietario.	Manual de procedimientos.	Registro de activos enviados a reubicados. Carteles de aviso.
	Vandalismo	Medio	Se debe contratar un seguro de robo o incendio para mitigar el daño de actos vandálicos y recuperar el negocio en el menor tiempo posible.	Contrato con Aseguradora.	Buscar compañías y bróker aseguradores. Seleccionar y contratar la compañía de seguros.

Fallas de equipos	Bajo	Deben protegerse los equipos de riesgos del medioambiente (por ejemplo, polvo, incendio y agua).	Proteger contra riesgos del medio ambiente.	Limpieza periódica de polvo. Adquisición de cobertores.
		Deben usarse reguladores de energía eléctrica en cada uno de los terminales y en los servidores deben usarse UPS	Instalación y uso de Reguladores de energía eléctrica	Adquirir reguladores. Adquirir UPS

2.4 ELABORACIÓN DE POLÍTICAS DE SEGURIDAD.

Una vez realizados los pasos anteriores, es posible definir la Política de seguridad de la información del cibercafé, tema de la monografía. Esta política está basada en la Norma UNE/ISO-IEC 27001 e inicia el proceso conocido como gestión de la seguridad de la información SGSI

La norma ISO, 27000 comprenden una serie de estándares como:

ISO/IEC27000 Sistemas de Gestión de Seguridad de la Información, Generalidades y vocabulario, publicada en Abril del 2009, en la que se recogen los términos y conceptos relacionados con la seguridad de la información, una visión general de la familia de estándares de esta área, una introducción a los SGSI, y una descripción del ciclo de mejora continua.

UNE-ISO/IEC 27001, Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos. (ISO/IEC 27001:2005), publicada en el año 2007. Esta es la norma fundamental de la familia, ya que contiene los requerimientos del sistema de gestión de seguridad de la información y es la norma con arreglo a la cual serán certificados los SGSI de las organizaciones que lo deseen.

ISO/IEC27002, Tecnología de la Información. Código de buenas prácticas para la Gestión de la Seguridad de la Información, publicada en el año 2005. Esta guía de buenas prácticas describe los objetivos de control y controles recomendables en cuanto a seguridad de la información.

ISO/IEC27003. Guía de implementación de SGSI e información acerca del uso del modelo PDCA y de los requerimientos de sus diferentes fases.

ISO27004: Estándar para la medición de la efectividad de la implantación de un SGSI y de los controles relacionados.

ISO/IEC27005:2008 Gestión del Riesgo en la Seguridad de la Información, publicada en el año 2008. Esta norma al pertenecer a la familia de las Normas 27000, se ajusta a las necesidades de las organizaciones que pretende realizar su análisis de riesgos en este ámbito y cumplir con los requisitos de la Norma ISO 27001.

ISO/IEC27006. Requisitos para las entidades que suministran servicios de auditoría y certificación de sistemas de gestión de seguridad de la información. Publicada en el año 2007. Recoge los criterios mediante los cuales una organización se puede acreditar para realizar esos servicios.

ISO/IEC27011. Directrices para la seguridad de la información en organizaciones de telecomunicaciones utilizando la Norma ISO/IEC 27002. Contiene recomendaciones para empresas de este sector, facilitando el cumplimiento de la Norma ISO27001 y conseguir un nivel de seguridad aceptable.

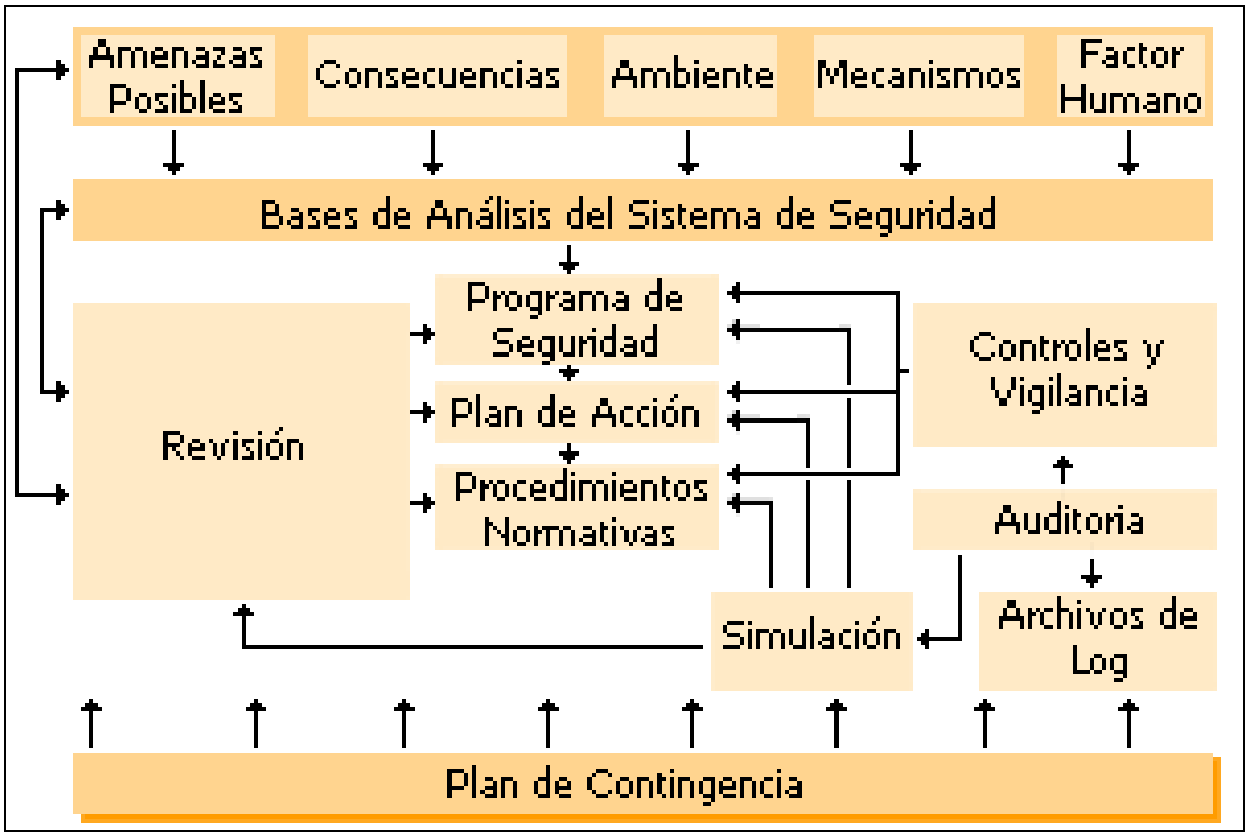
EN ISO27799. Gestión de la seguridad de la información sanitaria utilizando la Norma ISO/IEC27002 (ISO27799:2008). Vigente en nuestro país ya que ha sido ratificada por AENOR en agosto de 2008. Como en la anterior, es una guía sectorial que da cabida a los requisitos específicos de entorno sanitario.

La política de seguridad de la información (PSI) comprende:

- Alcance de la política, incluyendo sistemas y personal sobre el cual se aplica.
- Objetivos de la política y descripción clara de los elementos involucrados en su definición.
- Responsabilidad de cada uno de los servicios, recurso y responsables en todos los niveles de la organización.
- Responsabilidades de los usuarios con respecto a la información que generan y a la que tienen acceso.
- Requerimientos mínimos para la configuración de la seguridad de los sistemas al alcance de la política.
- Definición de violaciones y las consecuencias del no cumplimiento de la política.
- Por otra parte, la política debe especificar la autoridad que debe hacer que las cosas ocurran, el rango de los correctivos y sus actuaciones que permitan dar indicaciones sobre la clase de sanciones que se puedan imponer. Pero, no debe especificar con exactitud qué pasara o cuándo algo sucederá; ya que no es una sentencia obligatoria de la ley.
- Explicaciones comprensibles (libre de tecnicismos y términos legales pero sin sacrificar su precisión) sobre el porqué de las decisiones tomadas.

- Finalmente, como documento dinámico de la organización, deben seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes: crecimiento de la planta de personal, cambio en la infraestructura computacional, alta y rotación de personal, desarrollo de nuevos servicios, cambio o diversificación de negocios, etc.

Una propuesta de una forma de realizar una PSI adecuada puede apreciarse en el siguiente diagrama:



(Tomado de : .http://www.arcert.gov.ar Gráfico 9.2 - Fuente: Manual de Seguridad en Redes)

La finalidad de las políticas de seguridad de la información que se describen a continuación es proporcionar instrucciones específicas sobre cómo mantener más seguros todos los recursos conectados o no a la red de un cibercafé.

1. Responsabilidades.

Los siguientes entes son responsables:

Los usuarios llámense empleado y propietario, son responsables de cumplir con todas las políticas del Programa relativas a la seguridad informática y en particular:

1.1. Conocer y aplicar las políticas y procedimientos apropiados en relación al manejo de la información y de los sistemas informáticos.
1.2. No divulgar información confidencial del negocio a personas no autorizadas.
1.3. No permitir y no facilitar el uso de los sistemas informáticos del negocio a personas no autorizadas.
1.4. No utilizar los recursos informáticos (hardware, software o datos) y de telecomunicaciones (teléfono, fax) para otras actividades que no estén directamente relacionadas con el área del negocio.
1.5. Proteger meticulosamente su contraseña y evitar que sea vista por otros en forma inadvertida.
1.6. Seleccionar una contraseña robusta que no tenga relación obvia con el usuario, sus familiares, el grupo de trabajo, y otras asociaciones parecidas.
1.7. Reportar inmediatamente a su jefe inmediato cualquier evento que pueda comprometer la seguridad de la Institución y sus recursos informáticos, como por ejemplo contagio de virus, intrusos, modificación o pérdida de datos y otras actividades poco usuales.

2. Políticas de seguridad para activos.

Los computadores del cibercafé sólo deben usarse en un ambiente seguro. Se considera que un ambiente es seguro cuando se han implantado las medidas de control apropiadas para proteger el software, el hardware y los datos. Esas medidas deben estar acorde a la importancia de los datos y la naturaleza de riesgos previsibles.

2.1 Debe respetarse y no modificar la configuración de hardware y software.

2.2 No se permite fumar, comer o beber mientras se está usando un PC.

2.3 Deben protegerse los equipos de riesgos del medioambiente (por ejemplo, polvo, incendio y agua).

2.4 Deben usarse reguladores de energía eléctrica en cada uno de los terminales y en los servidores deben usarse UPS.

2.5 Cualquier falla en los computadores o en la red debe reportarse inmediatamente ya que podría causar problemas serios como pérdida de la información o indisponibilidad de los servicios.

2.6 Deben protegerse los equipos para disminuir el riesgo de robo, destrucción, y mal uso. Las medidas que se recomiendan incluyen el uso de vigilantes y cerradura con llave.

2.7 Los equipos deben marcarse para su identificación y control de inventario. Los registros de inventario deben mantenerse actualizados.

2.8 No pueden moverse los equipos o reubicarlos sin permiso. Para llevar un equipo fuera del cibercafé se requiere una autorización escrita del propietario.

2.9 La pérdida o robo de cualquier componente de hardware o programa de software debe ser reportada inmediatamente.

2.10 Para prevenir el acceso no autorizado, los usuarios del servidor deben usar un sistema de contraseñas robusto y además deben configurar el protector de pantalla para que se active al cabo de 15 minutos de inactividad y que requiera una contraseña al reasumir la actividad. Además el usuario debe activar el protector de pantalla manualmente cada vez que se ausente de su oficina.

2.11 Los datos confidenciales que aparezcan en la pantalla deben protegerse de ser vistos por otras personas mediante disposición apropiada del mobiliario de la oficina y protector de pantalla. Cuando ya no se necesiten o no sean de utilidad, los datos confidenciales se deben borrar.

2.12 A menos que se indique lo contrario, los usuarios deben asumir que todo el software del Cibercafé está protegido por derechos de autor y requiere licencia de uso. Por tal razón es ilegal y está terminantemente prohibido hacer copias o usar ese software para fines personales.

2.13 Debe instalarse y activarse una herramienta antivirus, la cual debe mantenerse actualizada. Si se detecta la presencia de un virus u otro agente potencialmente peligroso, se debe notificar inmediatamente al Administrador de Sistemas (en este caso el propietario) y poner el servidor o estación de trabajo en cuarentena hasta que el problema sea resuelto.

2.14 Debe utilizarse un programa antivirus para examinar todo software que venga de afuera o descargue.

2.15 No debe utilizarse software bajado de Internet en el servidor y en general software que provenga de una fuente no confiable, a menos que se haya sido comprobado en forma rigurosa y que esté aprobado su uso por el propietario.

2.16 Para prevenir demandas legales o la introducción de virus informáticos, se prohíbe estrictamente la instalación de software no autorizado, incluyendo el que haya sido adquirido por el propio usuario. Asimismo, no se permite el uso de software de distribución gratuita o shareware, a menos que haya sido previamente aprobado por el propietario.

2.17 Para ayudar a restaurar los programas originales no dañados o infectados, deben hacerse copias de todo software nuevo antes de su uso, y deben guardarse tales copias en un lugar seguro.

2.18 No deben usarse USB u otros medios de almacenamiento en cualquier computadora del cibercafé sin que antes hayan sido verificados que estén libres de virus u otros agentes dañinos.

2.19 Periódicamente debe hacerse el respaldo de los datos guardados en el servidor y las copias de respaldo deben guardarse en un lugar seguro, a prueba de hurto, incendio e inundaciones. Los programas y datos vitales para la operación del Cibercafé debe guardarse en otra sede, lejos del negocio.

2.20 La información del cibercafé clasificada como confidencial o de uso restringido, debe guardarse de forma segura.

2.21 Siempre que sea posible, deba eliminarse información confidencial de los computadores y unidades de disco duro antes de que les mande a reparar. Si esto no es posible, se debe asegurar que la reparación sea efectuada por empresas responsables, con las cuales se haya firmado un contrato de confidencialidad.

2.22 Se debe contratar un seguro de robo o incendio para mitigar el daño de actos vandálicos y recuperar el negocio en el menor tiempo posible.

3. Políticas de seguridad para las comunicaciones.

3.1 Propiedad de la información

Con el fin de mejorar la productividad del cibercafé se promueve el uso responsable de las comunicaciones en forma electrónica, en particular el teléfono, el correo de voz, el correo electrónico, y el fax. Los sistemas de comunicación y los mensajes generados y procesados por tales sistemas, incluyendo las copias de respaldo, se deben considerar como propiedad del cibercafé y no propiedad de los usuarios de los servicios de comunicación.

3.2. Uso de los sistemas de comunicación

3.2.1 Los sistemas de comunicación del cibercafé generalmente sólo deben usarse para actividades de trabajo. El uso personal en forma ocasional es permisible siempre y cuando consuma una cantidad mínima de tiempo y recursos, y además no interfiera con la productividad del negocio.

3.2.2 Se prohíbe el uso de los sistemas de comunicación para actividades comerciales privadas.

3.2.3 La navegación en Internet en el servidor para fines personales no debe hacerse a expensas del tiempo y recursos del negocio. En tal sentido, no deberán usarse las instalaciones y recursos del cibercafé para fines ajenos a lo laboral.

3.2.4 Se prohíbe el uso de aplicaciones y/o herramientas no permitidas que saturen los canales de comunicación del cibercafé, tales como gestores de descarga de archivos multimedia (audio y/o videos), Ares, Torrent entre otros.

3.2.5 Se restringe el uso de aplicativos de comunicación tipo chat (Facebook, Messenger, Skype y similares), su instalación deberá ser autorizada por el propietario.

3.3. Confidencialidad y privacidad.

3.3.1 Los recursos, servicios y conectividad disponibles vía Internet abren nuevas oportunidades, pero también introducen nuevos riesgos. En particular, no debe enviarse a través de Internet mensajes con información confidencial a menos que estén cifrada. Para tal fin debe utilizarse PGP (Pretty Good Privacy), Outlook, Outlook Express u otros productos previamente aprobados por Informática.

3.3.2. Es política del Cibercafé no monitorear regularmente las comunicaciones. Sin embargo, el uso y el contenido de las comunicaciones puede ocasionalmente ser supervisado en caso de ser necesario para actividades de mantenimiento, seguridad o auditoría. Puede ocurrir que el personal técnico vea el contenido de un mensaje de un empleado individual durante el curso de resolución de un problema.

3.3.3. De manera consistente con prácticas generalmente aceptadas, el propietario del negocio procesa datos estadísticos sobre el uso de los sistemas de comunicación. Como ejemplo, los reportes de la central telefónica, celulares contienen detalles

sobre el número llamado, la duración de la llamada, y la hora en que se efectuó la llamada.

3.4. Reenvío de mensajes

Tomando en cuenta que cierta información está dirigida a personas específicas y puede no ser apta para otros, dentro y fuera del Cibercafé, se debe ejercer cierta cautela al remitir los mensajes. En todo caso no debe remitirse información confidencial del Cibercafé sin la debida aprobación.

4. Políticas de seguridad para redes.

4.1. Propósito

El propósito de esta política es establecer las directrices, los procedimientos y los requisitos para asegurar la protección apropiada del Cibercafé al estar conectada a redes de computadoras.

4.2. Alcance

Esta política se aplica a todos los empleados, clientes y personal temporal del Cibercafé.

4.3. Aspectos generales

Es política del Cibercafé prohibir la divulgación, duplicación, modificación, destrucción, pérdida, mal uso, robo y acceso no autorizado de información propietaria. Además, es su política proteger la información que pertenece a otras empresas o personas y que le haya sido confiada.

4.4. Modificaciones

Todos los cambios en las bases celulares, en los servidores y equipos de red del Cibercafé, incluyendo la instalación de nuevo software, el cambio de direcciones IP, la reconfiguración de ruteadores y switchs, deben ser documentados y debidamente aprobados, excepto si se trata de una situación de emergencia. Todo esto es para evitar problemas por cambios apresurados y que puedan causar interrupción de las comunicaciones, caída de la red, denegación de servicio o acceso inadvertido a información confidencial.

4.5. Cuentas de los usuarios

4.5.1. Cuando un empleado recibe una nueva cuenta, debe firmar un documento donde declara conocer las políticas y procedimientos de seguridad, y acepta sus responsabilidades con relación al uso de esa cuenta.

4.5.2. La solicitud de una nueva cuenta o el cambio de privilegios debe ser hecha por escrito y debe ser debidamente aprobada.

4.5.3. No debe concederse una cuenta a personas que no sean empleados del Cibercafé a menos que estén debidamente autorizados, en cuyo caso la cuenta debe expirar automáticamente al cabo de un lapso de 30 días.

4.5.4. Privilegios especiales, tal como la posibilidad de modificar o borrar los archivos de otros usuarios, sólo deben otorgarse a aquellos directamente responsable de la administración o de la seguridad de los sistemas.

4.5.5. No deben otorgarse cuentas a técnicos de mantenimiento ni permitir su acceso remoto a menos que el Administrador de Sistemas determine que es necesario. En todo caso esta facilidad sólo debe habilitarse para el periodo de tiempo requerido para efectuar el trabajo (como por ejemplo, el mantenimiento remoto, daño del servidor).

4.5.6. Se prohíbe el uso de cuentas anónimas o de invitado (guest) y los usuarios deben entrar al sistema mediante cuentas que indiquen claramente su identidad.

4.5.7. Toda cuenta queda automáticamente suspendida después de un cierto periodo de inactividad. El periodo recomendado es de 30 días.

4.5.8. Cuando un usuario (empleado) renuncia, es despedido o se finiquita su contrato con el Cibercafé, debe desactivarse su cuenta antes de que deje el cargo.

4.6. Contraseñas y el control de acceso

4.6.1. El usuario no debe guardar su contraseña en una forma legible en archivos en disco, y tampoco debe escribirla en papel y dejarla en sitios donde pueda ser encontrada. Si hay razón para creer que una contraseña ha sido comprometida, debe cambiarla inmediatamente. No deben usarse contraseñas que son idénticas o substancialmente similares a contraseñas previamente empleadas. Siempre que sea posible, debe impedirse que los usuarios vuelvan a usar contraseñas anteriores.

4.6.2. Nunca debe compartirse la contraseña o revelarla a otros. El hacerlo expone al usuario a las consecuencias por las acciones que los otros hagan con esa contraseña.

4.6.3. Está prohibido el uso de contraseñas de grupo para facilitar el acceso a archivos, aplicaciones, bases de datos, computadoras, redes, y otros recursos del sistema. Esto se aplica en particular a la contraseña del administrador.

4.6.4. La contraseña inicial emitida a un nuevo usuario sólo debe ser válida para la primera sesión. En ese momento, el usuario debe escoger otra contraseña.

4.6.5. Las contraseñas predefinidas que traen los equipos nuevos tales como ruteadores, switchs, etc., deben cambiarse inmediatamente al ponerse en servicio el equipo.

4.6.6. Para prevenir ataques, cuando el software del sistema lo permita, debe limitarse a 3 el número de consecutivos de intentos infructuosos de introducir la contraseña, luego de lo cual la cuenta involucrada queda suspendida y se alerta al Administrador del sistema. Si se trata de acceso remoto vía módem por discado, la sesión debe ser inmediatamente desconectada.

4.6.7. Si no ha habido ninguna actividad en un terminal, PC o estación de trabajo durante un cierto periodo de tiempo, el sistema debe automáticamente borrar la pantalla y suspender la sesión. El periodo recomendado de tiempo es de 15 minutos. El re-establecimiento de la sesión requiere que el usuario proporcione se autentique mediante su contraseña (o utilice otro mecanismo, por ejemplo, tarjeta inteligente o de proximidad).

4.6.8. Si el sistema de control de acceso no está funcionando propiamente, debe rechazar el acceso de los usuarios hasta que el problema se haya solucionado.

4.6.9. Los usuarios no deben intentar violar los sistemas de seguridad y de control de acceso. Acciones de esta naturaleza se consideran violatorias de las políticas del Cibercafé, pudiendo ser causal de resolución de contrato o negación del servicio ofrecido.

4.6.10. Para tener evidencias en casos de acciones disciplinarias y judiciales, cierta clase de información debe capturarse, grabarse y guardarse cuando se sospeche que se esté llevando a cabo abuso, fraude u otro crimen que involucre los sistemas informáticos.

4.6.11. Los archivos de bitácora (logs) y los registros de auditoría (audit trails) que graban los eventos relevantes sobre la seguridad de los sistemas informáticos y las comunicaciones, deben revisarse periódicamente y guardarse durante un tiempo prudencial de por lo menos tres meses. Dicho archivos son importantes para la detección de intrusos, brechas en la seguridad, investigaciones, y otras actividades de auditoría. Por tal razón deben protegerse para que nadie los pueda alterar y que sólo los pueden leer las personas autorizadas.

4.6.12. Los servidores de red y los equipos de comunicación (bases celulares, ruteadores, etc.) deben estar ubicados en locales apropiados, protegidos contra daños y robo. Debe restringirse severamente el acceso a estos locales y a los cuartos de cableado a personas no autorizadas mediante el uso de cerraduras y otros sistemas de acceso.

CAPITULO III

ANÁLISIS

3.1. EVALUACIÓN DE LAS HERRAMIENTAS DE CONTROL Y SOFTWARE LIBRE

El proceso de evaluación de herramientas de control se realizó con el siguiente software:

- Kaspersky Internet Security V. 7.0.1.325
- GFI LANguard V 9.6
- Y en relación al software libre se evaluó:
- Elistara V.23.25
- SUPERAntiSpyware V.4

Según datos estadísticos consultados esta herramienta presenta para los usuarios las siguientes ventajas y desventajas:

Herramienta Kaspersky Internet Security

VENTAJAS	DESVENTAJAS
Fácil instalación y uso.	Análisis de correo no deseado no es eficiente.
Falso positivos bajos	Firewall hace lentos algunos procesos.
No es pesado	Uso de memoria RAM
Oferta de licencias gratuitas	No gratuito
Amplia detección y eliminación de virus.	Tiempo de limpieza
Manual de instrucciones	
Soporte de fábrica	
Costo estima $ 65	
Firewall	
Buena capacidad de actualización	

Herramienta Elistara.

VENTAJAS	DESVENTAJAS
Detecta spyware y adware	No es un antivirus
Detección de equipos ya infectados.	No protege el equipo.
Gratuita.	
Actualización constante	
Fácil instalación y descarga.	
No ocupa mucho espacio (aprox. 424Kb)	
No consume recursos	
Manual y soporte en internet.	

Herramienta GFI

VENTAJAS	DESVENTAJAS
Realiza la gestión de vulnerabilidades. Escanea, analiza y repara la red.	Requiere recursos mínimos de máquina como procesador 1GB, espacio en DD 1GB y memoria de 1GB.
Realiza gestión de parches de software.	No es gratuito.
Escanea puertos y servicios	
Elimina programas no autorizados.	
Utilizado para auditorias informáticas.	
Costo aprox. $320 por 1 año	

Herramienta SUPERAntiSpyware

VENTAJAS	DESVENTAJAS
Busca de spyware, troyanos, dialers, gusanos, adware.	No tiene protección en tiempo real gratuita, tiene un costo.
Impide la aparición de banners.	No debe utilizarse como única herramienta.
Elimina archivos de rastreo	No es un antivirus
Existen versiones gratuitas	
Fácil uso e instalación.	

3.2. IDENTIFICACIÓN DE CASOS DE USO.

Las herramientas evaluadas no son aplicables para todos los negocios o empresas, su uso depende de factores relacionados con el equipamiento y costo de cada una.

En nuestro medio la mayoría de empresas o negocios pequeños utilizan la herramienta Kaspersky Internet Security por ser una herramienta accesible y de bajo costo en comparación a otras herramientas. También ofrece una amplia gama de protección para la mayoría de amenazas sin requerir mayores recursos del equipo.

Sin embargo, herramientas como GFI, son aplicables para empresas medianas y grandes cuyo volumen y confidencialidad de la información en grande y vital como en un banco que es blanco de ataques de hackers.

Herramientas como Elistara y/o SUPERAntiSpyware, a pesar de ser livianas, de evaluación y gratuitas no ofrecen una protección segura para todas las amenazas como lo veremos más adelante.

3.3. ANÁLISIS DE LA SOLUCIÓN.

Como ya se mencionó en el capítulo anterior, la implementación de una o varias herramientas dependen de las características de los equipos de una empresa o negocio y del factor económico. Si bien es cierto que la implementación de todas las herramientas brindarían un amplio espectro de protección, también es cierto que no son aplicables todo el tiempo, ni en todos los casos.

La solución más recomendable para el negocio tema de esta monografía, es continuar con el uso de la herramienta Kaspersky Internet Security y la implementación de las políticas de seguridad. Utilizando las herramientas Elistara y/o SUPERAntiSpyware como complemento de detección de amenazas a través de la implementación de análisis periódicos.

Para este caso no sería viable la adquisición de la herramienta en primer lugar por el costo y en segundo por la naturaleza del negocio no requiere su implementación. Sin embargo se sugiere utilizar esta herramienta en versiones de evaluación para detectar problemas de red en forma periódica.

CAPITULO IV

DESARROLLO DEL PLAN DE IMPLEMENTACIÓN

El plan de implementación hace referencia a las medidas a adoptarse a corto, mediano y largo plazo, mismas que tiene relación directa con la SGSI gestión de políticas de la seguridad de la información, ya expuestas en el capítulo anterior, siendo las siguientes las sugerencias a implementarse en el cibercafé:

CORTO PLAZO

Socialización de la política de seguridad de la información del cibercafé con el propietario y empleado.

Inventario.

Contrato de confidencialidad.

Control de acceso por usuario.

Medidas de protección contra riesgo del medio ambiente.

Implementación de herramientas antivirus, Anti-Spy y Firewall en el servidor del negocio, se instalará Elistara, Spyboot, Karpersky.

Implementación de una contraseña robusta siguiendo lineamientos como combinación de caracteres, extensión y actualización periódica.

Implementación de cableado eléctrico adecuado, cambiando las extensiones, colocando de manera ordenada los reguladores de forma que no impidan u obstaculicen el paso dentro del negocio.

Respaldo de información.

Implementación de medidas de seguridad del sistema operativo como protectores de pantalla.

MEDIANO PLAZO

Implementar medidas de seguridad: uso de vigilancia como la instalación de cámaras de seguridad.

Manual de procedimientos: documentar el manejo del negocio.

Reubicación de activos.

Contrato con Aseguradora

LARGO PLAZO

Plan de contingencia para mitigar los riesgos luego de que estos sucedan.

Licenciamiento, adquisición de herramientas de Windows XP y Microsoft Office 2007.

Firewall físico como por ejemplo IPCOP.

Cambio de sistema operativo, a uno de distribución gratuita como Linux.

Reingeniería del negocio, implementación de un servidor Linux, con terminales Win XP.

CAPITULO V

PRUEBAS DEL SOFTWARE

5.1. INSTALACIÓN Y CONFIGURACIÓN DEL SERVIDOR LOCAL.

La fase práctica de la presente monografía, se inicia con la configuración de una máquina de prueba en la que se van a simular ataques de virus, que son los más comunes en un cibercafé, se procedió a realizar los siguientes pasos:

- Se formateo el Disco Duro de la máquina de prueba.
- Se procedió a instalar el sistema operativo Windows XP.
- Actualización de Win XP, KB898461. Installer 3.1
- Se configuro el acceso a la red local.
- Se instalaron los siguientes programas para probar un ataque de virus: Microsoft Office 2003, ares.
- Se desactivo el bloqueador de elementos emergentes.

Una vez instalados se procedió a realizar trabajos comunes que se dan en el negocio de un cibercafé como: escribir textos, ingresar a google, bajar música, jugar por internet, acceder a redes sociales como facebook, Hi5, Twitter, messanger entre otros y grabar archivos de trabajos en general.

Es importante anotar, que también los clientes/usuarios de un cibercafé, traen dispositivos de almacenamiento como USB, que pueden estar contaminados por virus que pueden a su vez ser trasmitidos a la máquina de prueba.

También se procedió a instalar un programa de internet para emoticones Iminent, el cual instaló una barra de herramientas en el explorador. Se accedió al sitio web: www.taringa.com, http://www.taringa.net/posts/downloads/8211326/Kaspersky-2011-_Crack.html

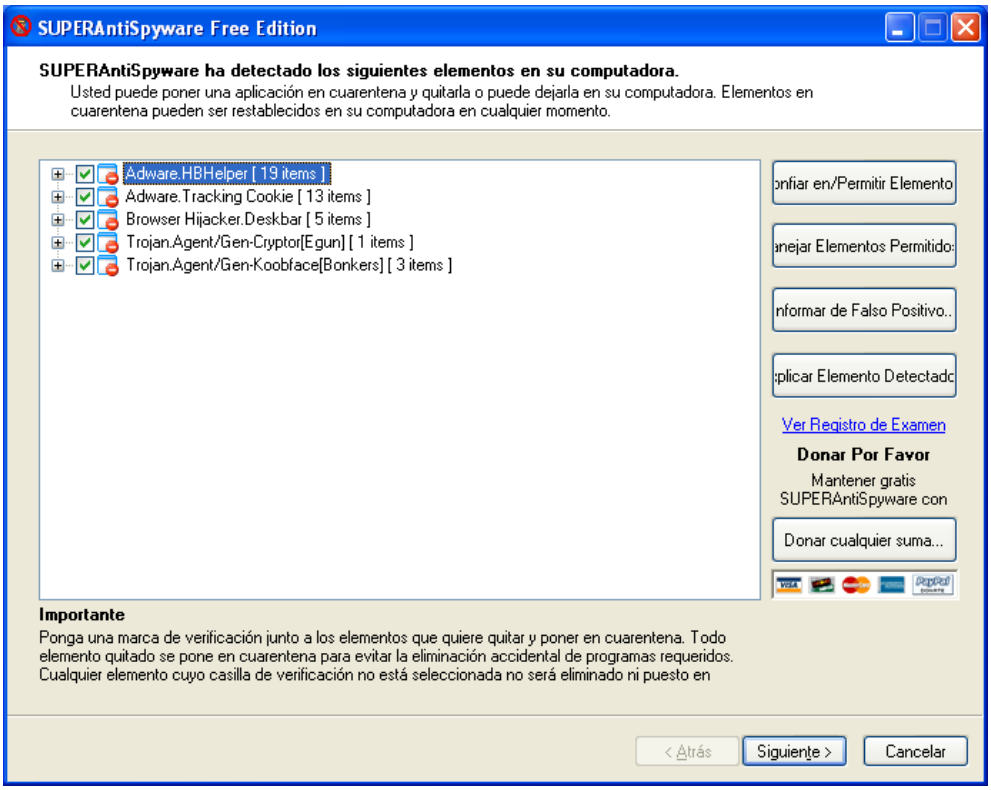
Todo esto provocó infección en la computadora, haciéndola más lenta e incluso provocó de otros medios de almacenamiento que no estaban contaminados. También el explorador empezó a dar problemas procediéndose a instalar el explorador 8, se crearon virus de carpetas de acceso directo y contaminaron varios dispositivos de almacenamiento, el menssanger perdió conexión,

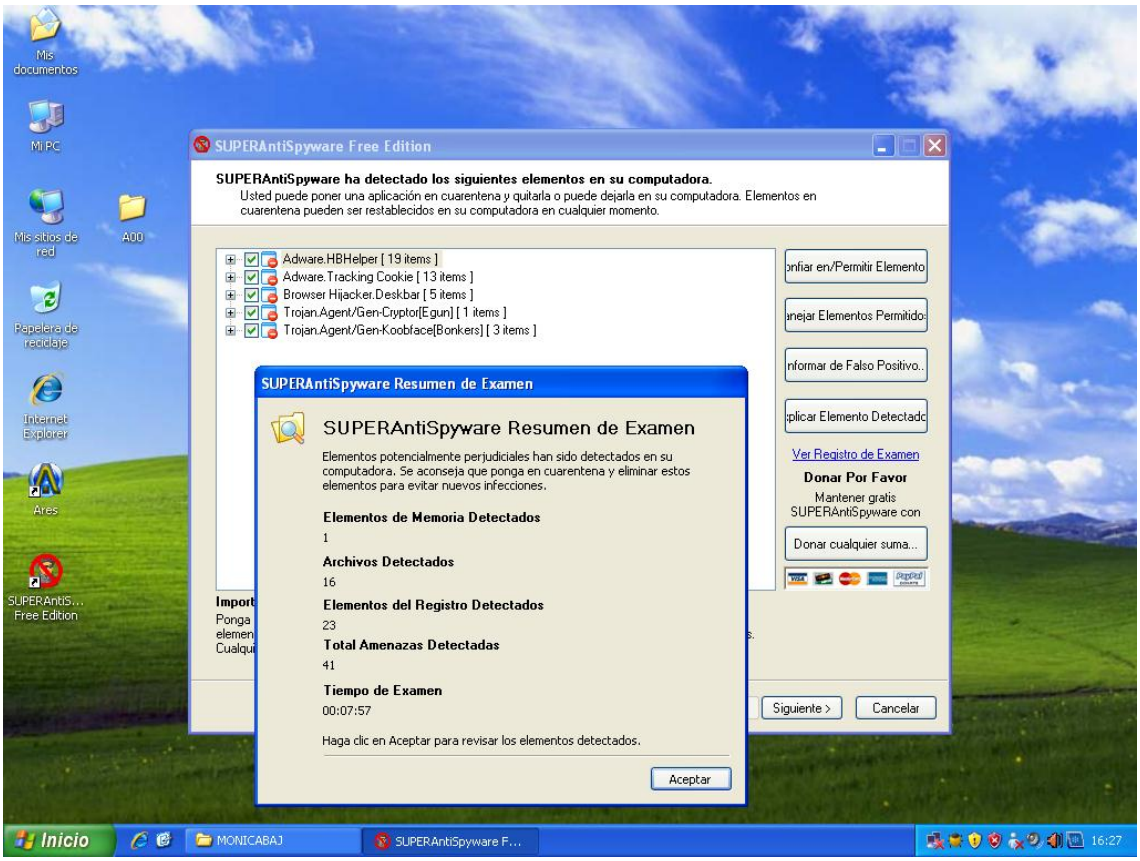
5.2. PRUEBAS DE SEGURIDAD.

Las pruebas de seguridad se realizaron en la máquina de pruebas de la siguiente forma:

- Se instalaron los siguientes programas: Elistara, Ani-Spy, Karpersky, GFI en modalidad de detección y no de eliminación para realizar una evaluación de las herramientas
- También se insertó un dispositivo de almacenamiento USB, infectado.

Obteniéndose los siguientes resultados:





Scan Log

http://www.superantispyware.com

Generated 05/19/2011 at 04:24 PM

Application Version : 4.52.1000

Core Rules Database Version : 7022

Trace Rules Database Version: 4834

Scan type : Complete Scan

Total Scan Time : 00:07:57

Memory items scanned : 430

Memory threats detected : 1

Registry items scanned : 5449

Registry threats detected : 24

File items scanned : 8594

File threats detected : 16

Trojan.Agent/Gen-Koobface[Bonkers]

C:\DOCUMENTS AND SETTINGS\MONICA\DATOS DE PROGRAMA\SERVICES.EXE

C:\DOCUMENTS AND SETTINGS\MONICA\DATOS DE PROGRAMA\SERVICES.EXE

C:\WINDOWS\Prefetch\SERVICES.EXE-1C1DD1E9.pf

Trojan.Agent/Gen-Cryptor[Egun]

[MSconfig] C:\DOCUMENTS AND SETTINGS\MONICA\DATOS DE PROGRAMA\SERVICES.EXE

Adware.HBHelper

HKLM\Software\Classes\CLSID\{CA3EB689-8F09-4026-AA10-B9534C691CE0}

HKCR\CLSID\{CA3EB689-8F09-4026-AA10-B9534C691CE0}

HKCR\CLSID\{CA3EB689-8F09-4026-AA10-B9534C691CE0}

HKCR\CLSID\{CA3EB689-8F09-4026-AA10-B9534C691CE0}\InprocServer32

HKCR\CLSID\{CA3EB689-8F09-4026-AA10-B9534C691CE0}\InprocServer32#ThreadingModel

HKCR\CLSID\{CA3EB689-8F09-4026-AA10-B9534C691CE0}\ProgID

HKCR\CLSID\{CA3EB689-8F09-4026-AA10-B9534C691CE0}\TypeLib

HKCR\CLSID\{CA3EB689-8F09-4026-AA10-B9534C691CE0}\VersionIndependentProgID

HKCR\URLSearchHook.ToolbarURLSearchHook.1

HKCR\URLSearchHook.ToolbarURLSearchHook.1\CLSID

HKCR\URLSearchHook.ToolbarURLSearchHook

HKCR\URLSearchHook.ToolbarURLSearchHook\CLSID

HKCR\TypeLib\{4509D3CC-B642-4745-B030-645B79522C6D}

HKCR\TypeLib\{4509D3CC-B642-4745-B030-645B79522C6D}\1.0

HKCR\TypeLib\{4509D3CC-B642-4745-B030-645B79522C6D}\1.0\0

HKCR\TypeLib\{4509D3CC-B642-4745-B030-645B79522C6D}\1.0\0\win32

HKCR\TypeLib\{4509D3CC-B642-4745-B030-645B79522C6D}\1.0\FLAGS

HKCR\TypeLib\{4509D3CC-B642-4745-B030-645B79522C6D}\1.0\HELPDIR

C:\ARCHIVOS DE PROGRAMA\IMINENT TOOLBAR\TBHELPER.DLL

Adware.Tracking Cookie

C:\Documents and Settings\MONICA\Cookies\monica@invitemedia[2].txt

C:\Documents and Settings\MONICA\Cookies\monica@ad.yieldmanager[2].txt

C:\Documents and Settings\MONICA\Cookies\monica@ak[2].txt

C:\Documents and Settings\MONICA\Cookies\monica@content.yieldmanager[1].txt

C:\Documents and Settings\MONICA\Cookies\monica@ads.pubmatic[1].txt

C:\Documents and Settings\MONICA\Cookies\monica@atdmt[2].txt

C:\Documents and Settings\MONICA\Cookies\monica@doubleclick[1].txt

C:\Documents and Settings\MONICA\Cookies\monica@weborama[1].txt

C:\Documents and Settings\MONICA\Cookies\monica@1050556762[2].txt

C:\Documents and Settings\MONICA\Cookies\monica@ads.ad4game[2].txt

C:\Documents and Settings\MONICA\Cookies\monica@AdClickTrackerServlet[2].txt

C:\Documents and Settings\MONICA\Cookies\monica@banners[2].txt

C:\Documents and Settings\MONICA\Cookies\monica@adServe[1].txt

Browser Hijacker.Deskbar

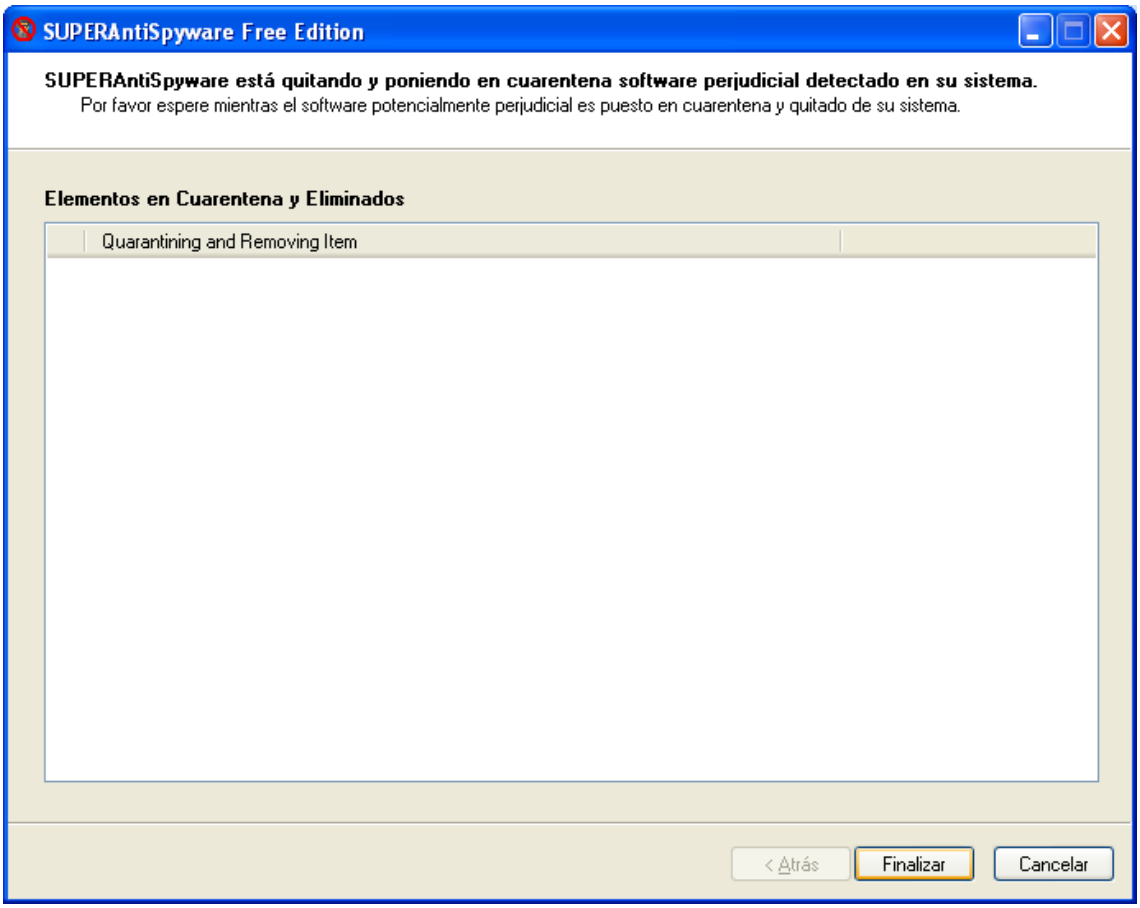
HKCR\Interface\{4897BBA6-48D9-468C-8EFA-846275D7701B}

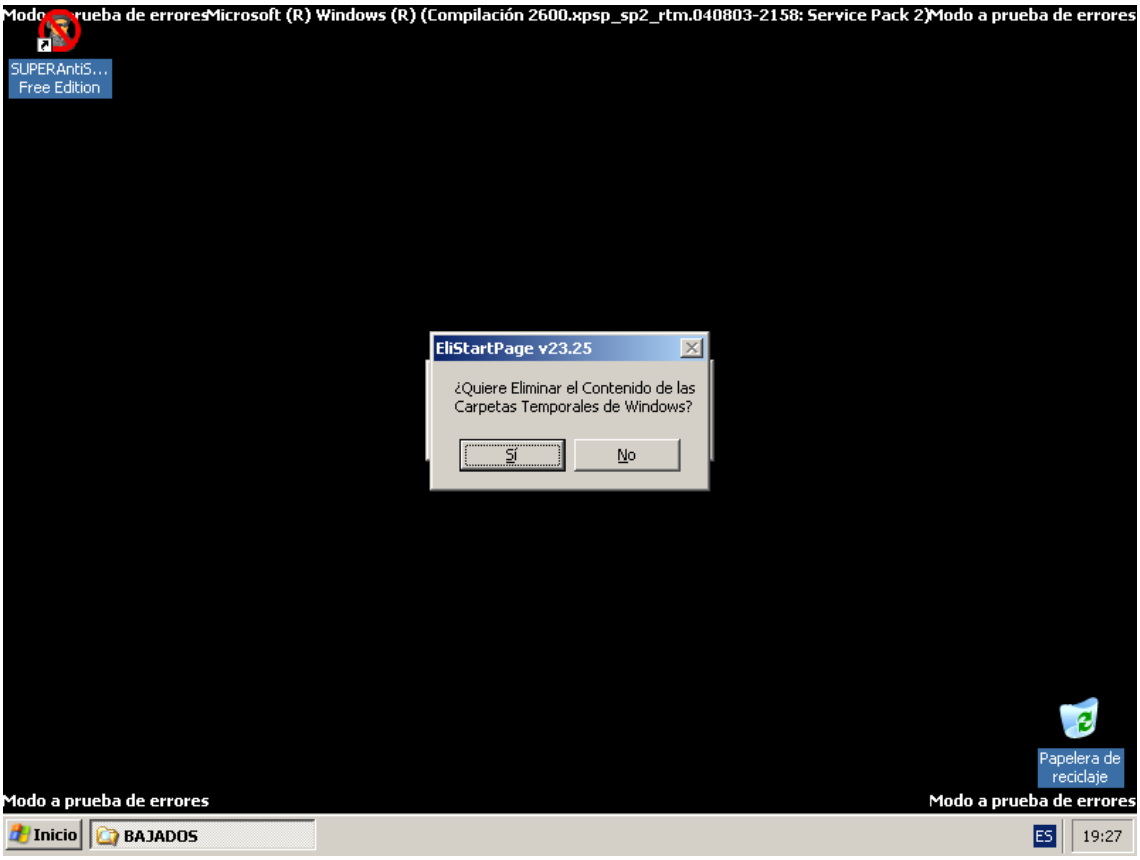
HKCR\Interface\{4897BBA6-48D9-468C-8EFA-846275D7701B}\ProxyStubClsid

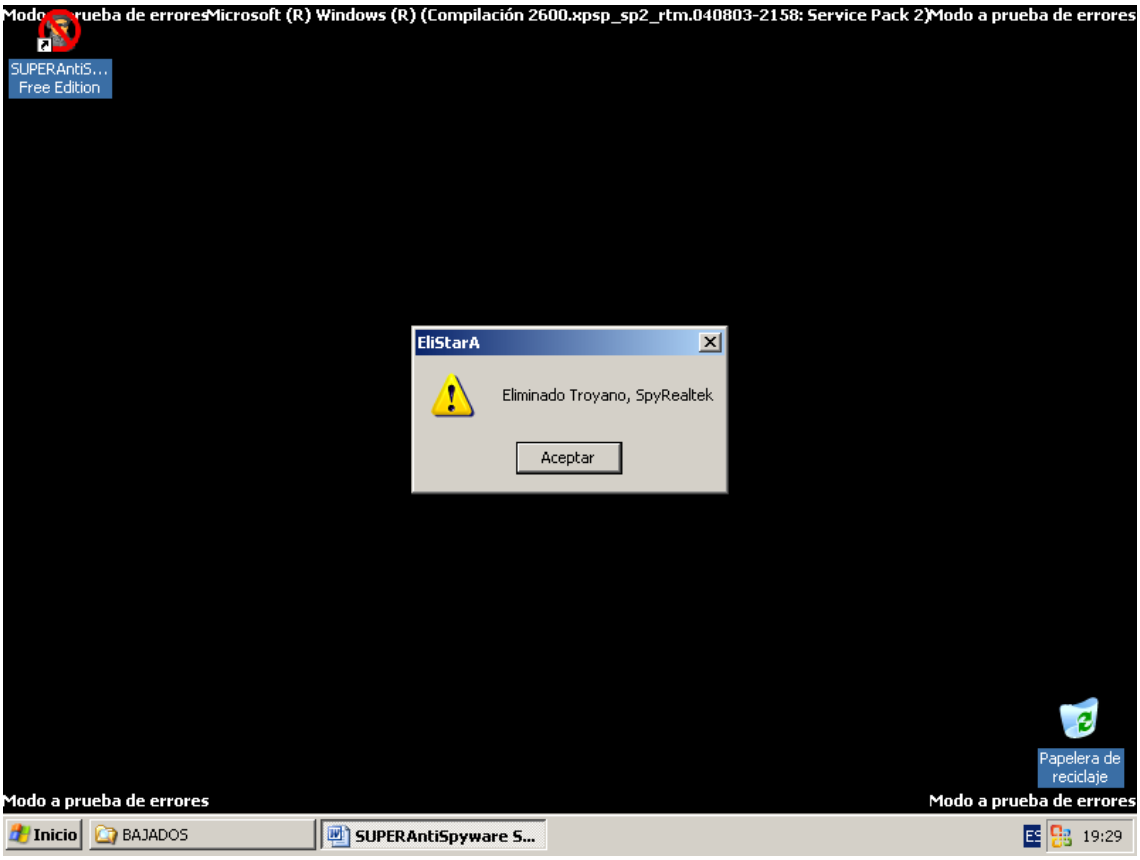
HKCR\Interface\{4897BBA6-48D9-468C-8EFA-846275D7701B}\ProxyStubClsid32

HKCR\Interface\{4897BBA6-48D9-468C-8EFA-846275D7701B}\TypeLib

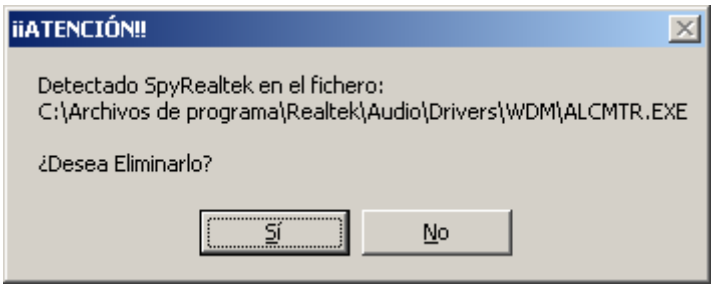
HKCR\Interface\{4897BBA6-48D9-468C-8EFA-846275D7701B}\TypeLib#Version

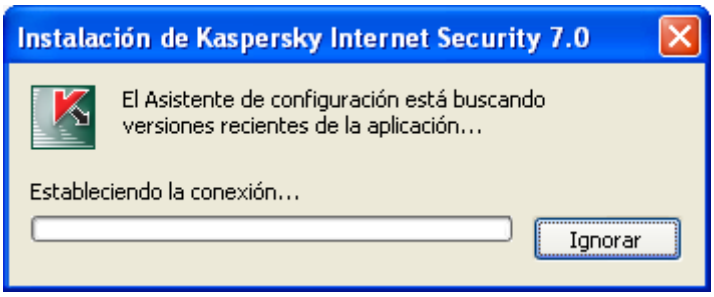


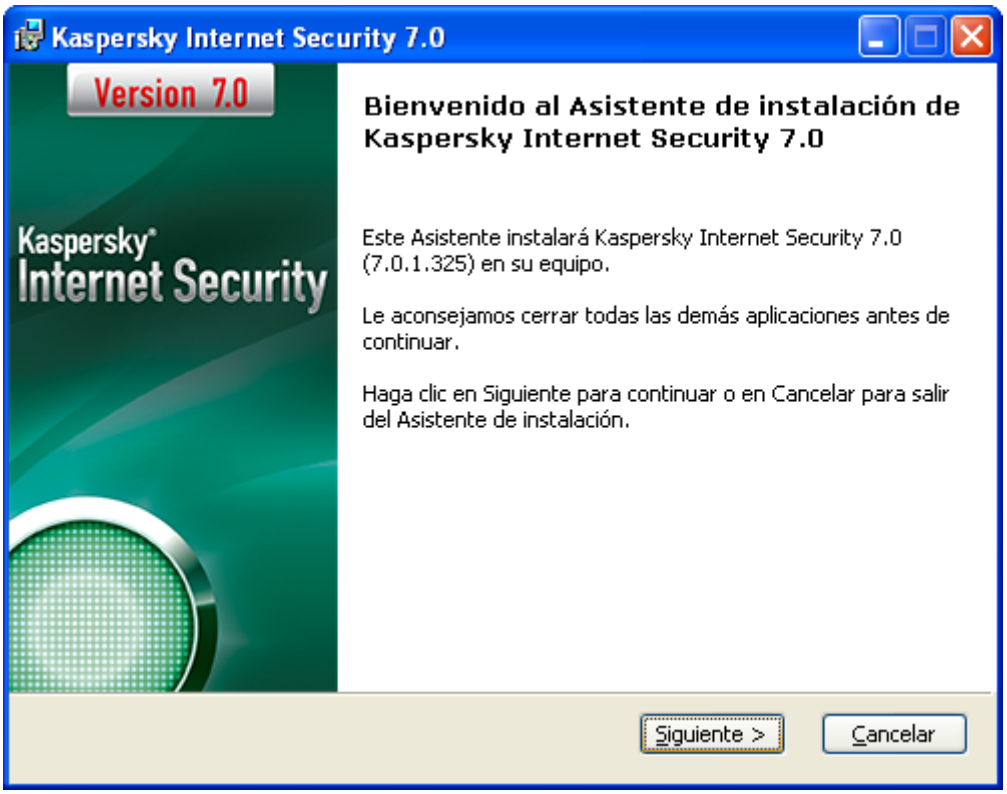

Modo a prueba de errores
Microsoft (R) Windows (R) (Compilación 2600.xpsp_sp2_rtm.040803-2158: Service Pack 2)
Modo a prueba de errores
SUPERAntiS...
Free Edition
EliStartPage v23.25
¿Quiere Eliminar el Contenido de las Carpetas Temporales de Windows?
Sí
No
Papelera de reciclaje
Modo a prueba de errores
Modo a prueba de errores
Inicio
BAJADOS
ES
19:27

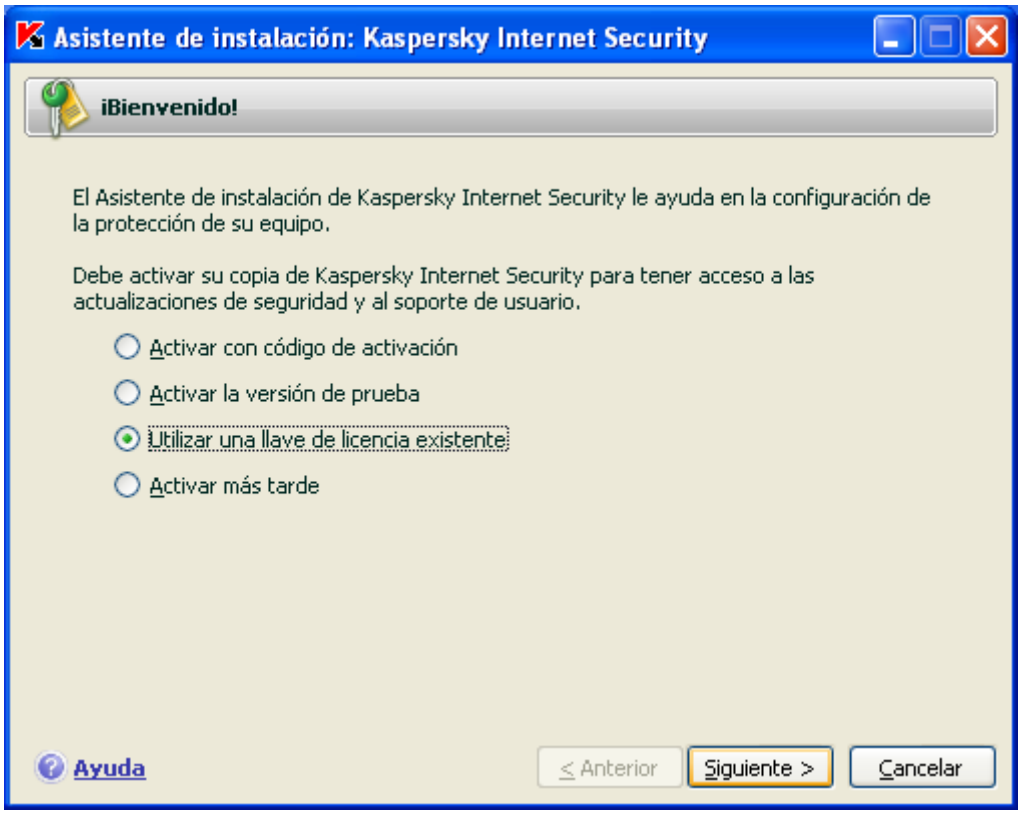

Modo a prueba de errores
Microsoft (R) Windows (R) (Compilación 2600.xpsp_sp2_rtm.040803-2158: Service Pack 2)
Modo a prueba de errores
SUPERAntiS...
Free Edition
EliStarA
Eliminado Troyano, SpyRealtek
Aceptar
Papelera de reciclaje
Modo a prueba de errores
Modo a prueba de errores
Inicio
BAJADOS
SUPERAntiSpyware S...
ES
19:29

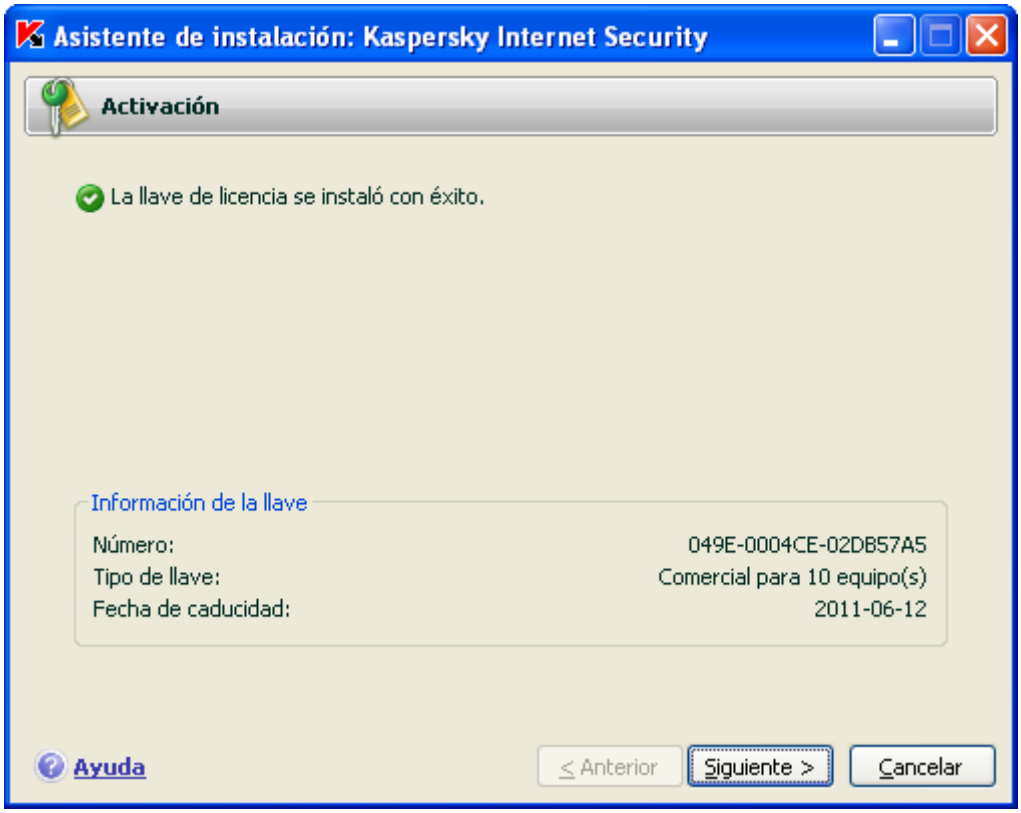

EliStarA
SATINFO
EliStartPage v23.25 (c)2011 S.G.H. / Satinfo S.L.
(www.satinfo.es)
Carpeta: C:\
Explorar
Salir
Seleccionar Carpeta
Estadísticas
Nº total de Directorios: 0
Nº total de Ficheros: 0
Nº de ficheros Analizados: 0
Nº de ficheros Infectados: 0
Nº de ficheros Eliminados: 0
Tiempo Transcurrido:
15295 Cadenas Víricas.
¡¡ATENCIÓN!!
Se aconseja desactivar temporalmente el residente del AntiVirus,
para que la exploración sea mas rapida.
Eliminar Ficheros Automaticamente
Mirar ZIPs

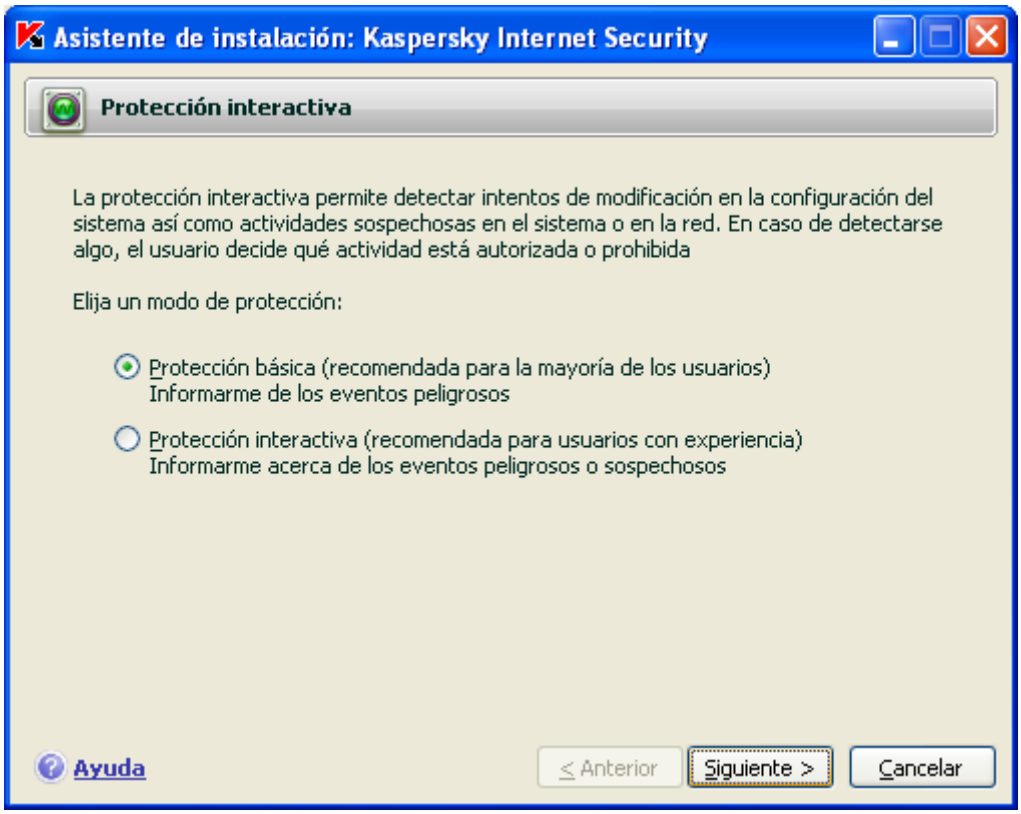

¡¡ATENCIÓN!!
Detectado SpyRealtek en el fichero:
C:\Archivos de programa\Realtek\Audio\Drivers\WDM\ALCMTR.EXE
¿Desea Eliminarlo?
Sí
No

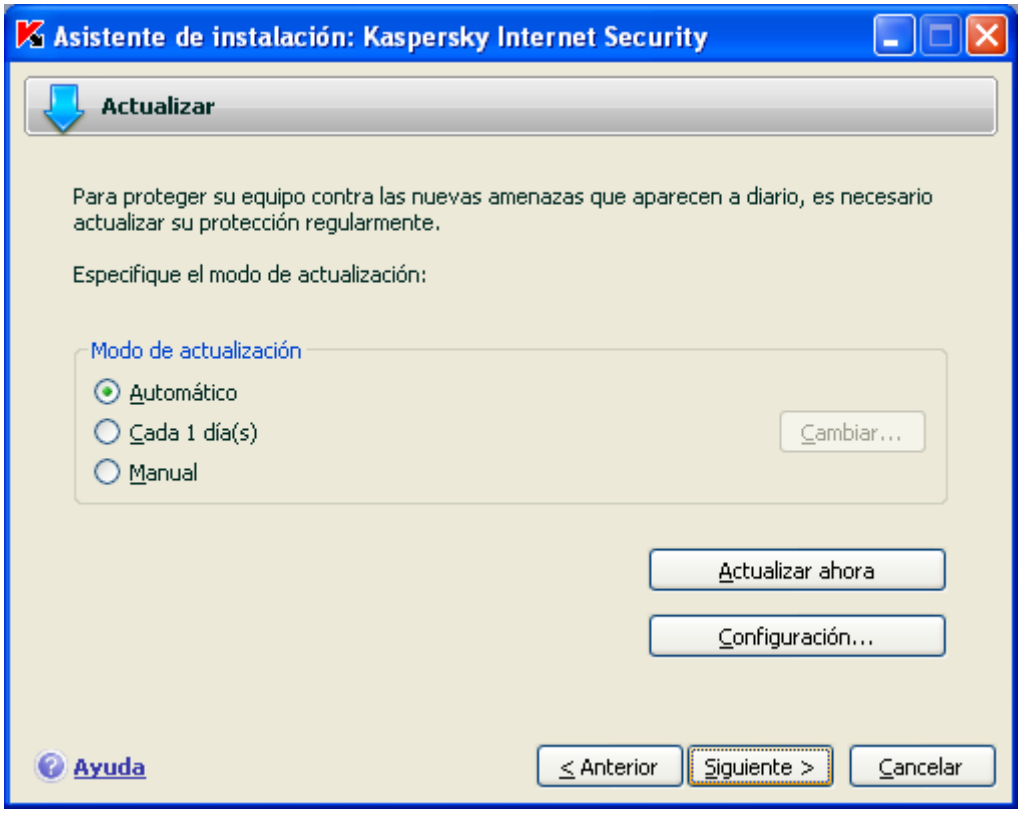

Instalación de Kaspersky Internet Security 7.0
El Asistente de configuración está buscando versiones recientes de la aplicación...
Estableciendo la conexión...
Ignorar

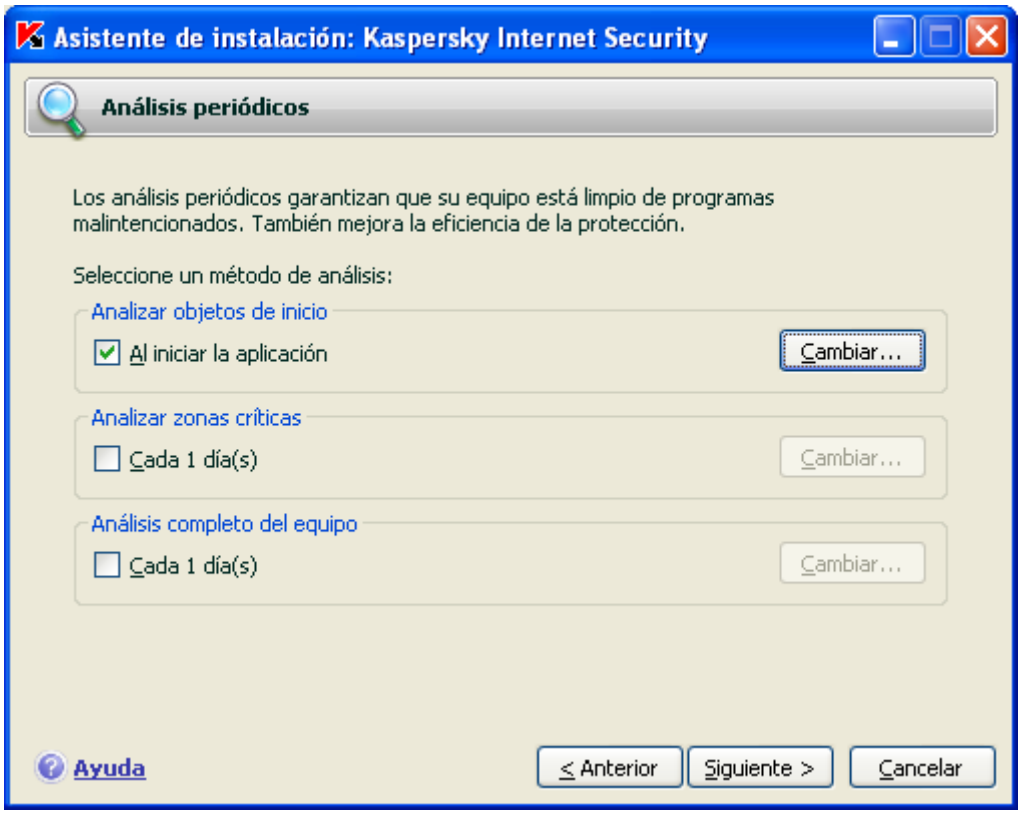

Kaspersky Internet Security 7.0
Version 7.0
Kaspersky
Internet Security
Bienvenido al Asistente de instalación de Kaspersky Internet Security 7.0
Este Asistente instalará Kaspersky Internet Security 7.0 (7.0.1.325) en su equipo.
Le aconsejamos cerrar todas las demás aplicaciones antes de continuar.
Haga clic en Siguiente para continuar o en Cancelar para salir del Asistente de instalación.
Siguiente >
Cancelar

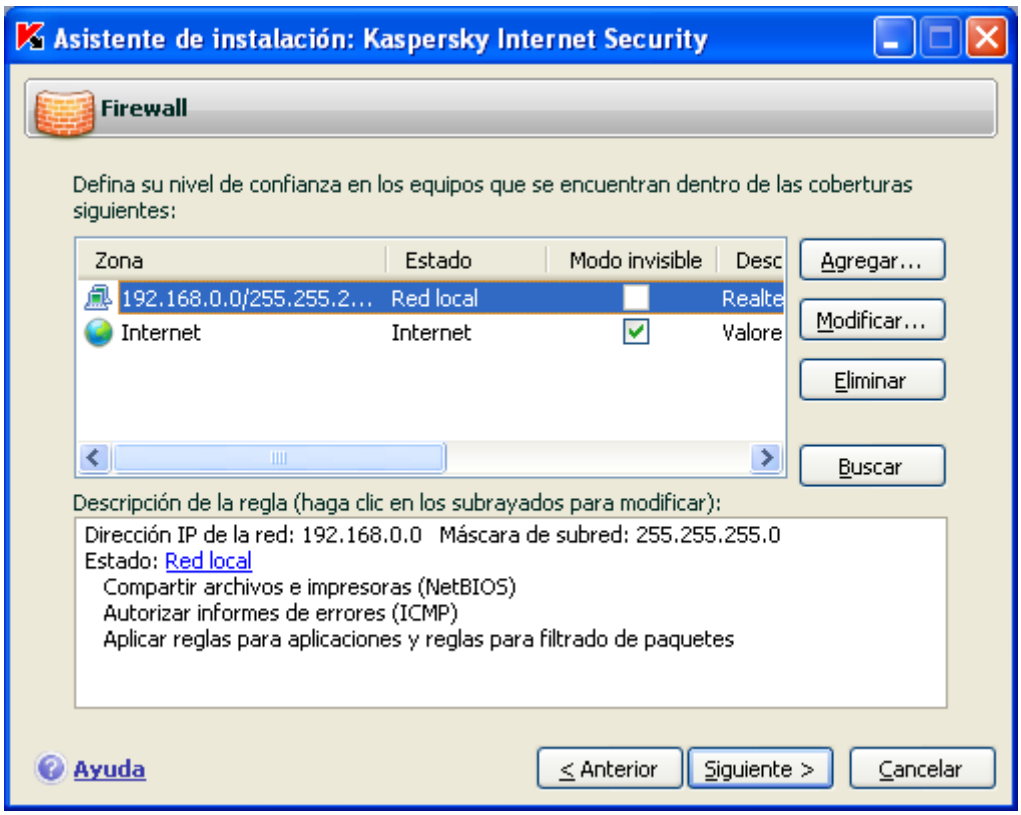

Asistente de instalación: Kaspersky Internet Security
¡Bienvenido!
El Asistente de instalación de Kaspersky Internet Security le ayuda en la configuración de la protección de su equipo.
Debe activar su copia de Kaspersky Internet Security para tener acceso a las actualizaciones de seguridad y al soporte de usuario.
Activar con código de activación
Activar la versión de prueba
Utilizar una llave de licencia existente
Activar más tarde
Ayuda
< Anterior
Siguiente >
Cancelar


Asistente de instalación: Kaspersky Internet Security
Activación
La llave de licencia se instaló con éxito.
Información de la llave
Número: 049E-0004CE-02DB57A5
Tipo de llave: Comercial para 10 equipo(s)
Fecha de caducidad: 2011-06-12
Ayuda
< Anterior
Siguiente >
Cancelar


Asistente de instalación: Kaspersky Internet Security
Protección interactiva
La protección interactiva permite detectar intentos de modificación en la configuración del sistema así como actividades sospechosas en el sistema o en la red. En caso de detectarse algo, el usuario decide qué actividad está autorizada o prohibida
Elija un modo de protección:
Protección básica (recomendada para la mayoría de los usuarios)
Informarme de los eventos peligrosos
Protección interactiva (recomendada para usuarios con experiencia)
Informarme acerca de los eventos peligrosos o sospechosos
Ayuda
< Anterior
Siguiente >
Cancelar


Asistente de instalación: Kaspersky Internet Security
Actualizar
Para proteger su equipo contra las nuevas amenazas que aparecen a diario, es necesario actualizar su protección regularmente.
Especifique el modo de actualización:
Modo de actualización
Automático
Cada 1 día(s)
Manual
Cambiar...
Actualizar ahora
Configuración...
Ayuda
< Anterior
Siguiente >
Cancelar


Asistente de instalación: Kaspersky Internet Security
Análisis periódicos
Los análisis periódicos garantizan que su equipo está limpio de programas malintencionados. También mejora la eficiencia de la protección.
Seleccione un método de análisis:
Analizar objetos de inicio
Al iniciar la aplicación
Cambiar...
Analizar zonas críticas
Cada 1 día(s)
Cambiar...
Análisis completo del equipo
Cada 1 día(s)
Cambiar...
Ayuda
< Anterior
Siguiente >
Cancelar


Asistente de instalación: Kaspersky Internet Security
Firewall
Defina su nivel de confianza en los equipos que se encuentran dentro de las coberturas siguientes:
Zona
Estado
Modo invisible
Desc
192.168.0.0/255.255.2...
Red local
Realte
Internet
Internet
Valore
Agregar...
Modificar...
Eliminar
Buscar
Descripción de la regla (haga clic en los subrayados para modificar):
Dirección IP de la red: 192.168.0.0 Máscara de subred: 255.255.255.0
Estado: Red local
Compartir archivos e impresoras (NetBIOS)
Autorizar informes de errores (ICMP)
Aplicar reglas para aplicaciones y reglas para filtrado de paquetes
Ayuda
< Anterior
Siguiente >
Cancelar


Asistente de instalación: Kaspersky Internet Security
Firewall
Aplicaciones de red
Se detectaron 41 aplicaciones de red. Kaspersky Internet Security ha creado reglas de autorización para estas aplicaciones, de acuerdo con su tipo.
Haga clic en "Aplicaciones..." para ver las aplicaciones y las reglas correspondientes.
Aplicaciones...
Protección avanzada
Para evitar la pérdida de datos, se recomienda desactivar la caché local de nombres de dominio (servicio caché de DNS).
Advertencia. Desactivar el servicio de caché DNS puede interferir en el funcionamiento de programas con conexiones de red múltiples (por ejemplo, clientes que comparten archivos).
Desactivar la caché de DNS
Ayuda
< Anterior
Siguiente >
Cancelar


Asistente de instalación: Kaspersky Internet Security
Finalizando la instalación
Instalación terminada
Debe reiniciar el equipo para completar la instalación.
Reiniciar el equipo
Ayuda
< Anterior
Terminar
Cancelar

A continuación se volvieron a ejecutar las herramientas mencionadas pero con la opción de eliminación, mejorando en un 60% su rendimiento de equipo en comparación con su rendimiento anterior. No mejoró a un 100%, pero se evito la amenaza de que se convierta en un foco de infección.

Como se pudo observar cada herramienta probada, detectó una amenaza diferente, pidiéndose concluir que la aplicación de estas 3 herramientas nos darían una amplio margen de protección, más no al 100% debido a que en seguridad informática no existe este término.

CAPITULO VI

CONCLUSIONES Y RECOMENDACIONES

Luego del trabajo realizado, tanto teórico como práctico, es importante concluir que la implementación de gestión de la seguridad de la información SGSI, constituye en la actualidad una herramienta indispensable para el óptimo manejo de una empresa o negocio (por más pequeño que este sea, como el caso del cibercafé tema de estudio).

Su gestión permite tener una visión clara de la información que se maneja dentro de una empresa o negocio, su importancia y los puntos que constituyen riesgos, que en muchas ocasiones sin esta gestión, llegan a ser descocidos y desvalorizados por los propietarios.

También podemos indicar que el solo conocimiento; es decir; tener un papel sobre la implementación de políticas para la seguridad de la información de un negocio, no bastan, es necesario también tomar conciencia de la importancia de su aplicación en el contexto actual y en relación a la naturaleza del negocio, de los riesgos inherentes a los avances tecnológicos y que esto conlleva a una constante investigación y actualización de las mejores herramientas antivirus, anti-spy, entre otras; y por ende implican el análisis de inversión económica en este rubro.

Muchas de estas herramientas mencionadas en esta monografía, pertenecen a una tecnología GNU, que abarataría costos, mientras que otras dependiendo de la naturaleza de la empresa o negocio requieren un análisis de costos versus su utilidad real; en relación a las características de su hardware y al factor económico.

Por ello se destaca y recomienda la implementación de una SGIS (gestión de la seguridad de la información), para asegurar el funcionamiento de una empresa bajo los parámetros que recomienda la seguridad de la información para una empresa o negocio. Se recomienda la implementación urgente de las medidas a corto plazo y se sugiere el lapso de 1 a 2 años la implementación de las medidas de seguridad a mediano y largo plazo. Tomando en consideración que una política de la seguridad de la información es atemporal y debe adecuarse a los avances tecnológicos y cambios y/o necesidades requerimientos de un negocio o empresa.

BIBLIOGRAFÍA

CERINI MARÍA DORELES, PRÁ PABLO IGNACIO. "Plan de Seguridad Informática", Director: Spesso Aldo. Universidad Católica de Córdova. Facultad de Ingeniería. Córdova. Argentina. Octubre 2002.

COHN MUROY DENNIS STEPHEN. "Análisis, Diseño e Implementación de una aplicación para la administración de las herramientas de seguridad en una red local". Director: Ing. Daly Scaletti Corrado. Universidad Católica del Perú. Facultad de Ciencias e Ingeniería. Lima. Perú. 2006.

GAVILANEZ BERREZUETA, PATRICIO EDUARDO; ULLOA FLORES, MARIA BERNARDA. "Seguridad de Redes". Director: s.d. Universidad del Azuay. Facultad de Ciencias de la Administración. Escuela de Ingeniería de Sistemas. Cuenca. 2004. 40 p. Ilus. Es.

GONZALEZ ZUBIETA, JOSE MARIA. PIATTINI, MARIO GERARDO; PESO NAVARRO, EMILIO DEL; COORD. Metodologías de control interno, seguridad y auditoría informática/ Auditoría informática: un enfoque práctico. Alfaomega. México. 2 ed. 2001. 660 p. pp. 45-92. ilus., grafs., tabs. Es.

RAMOS GONZALEZ, MIGUEL ANGEL. PIATTINI, MARIO GERARDO; PESO NAVARRO, EMILIO DEL; COORD. Auditoría de la seguridad/ Auditoría informática: un enfoque práctico/ Alfaomega. México. 2 ed. 2001. 660 p. pp. 389 - 422. ilus., grafs., tabs. Es.

VILLENA AGUILAR MOISES ANTONIO. "Sistema de gestión de seguridad de información para una Institución financiera". Director: s.d. Pontificia Universidad Católica del Perú. Facultad de Ciencias e Ingeniería. Lima. Perú. Octubre 2008.

"**AV-Comparatives.org** ". http://www.av-comparatives.org/ [consulta 14 de diciembre de 2011]

http://www.zonavirus.com/imagenes-antivirus-virus/cabecera/logo-zonavirus.png [consulta 14 de diciembre de 2011]

http://www.zonavirus.com/descargas/descargar-elistara.asp [consulta 14 de diciembre de 2011]

SUPERAntiSpyware.com Remove Malware Remove Spyware - AntiMalware, AntiSpyware, AntiAdware!.htm http://www.superantispyware.com/onlinescan.html

http://latam.kaspersky.com/ [consulta 14 de diciembre de 2011]

http://latam.kaspersky.com/productos/antivirus-online-gratis [consulta 14 de diciembre de 2011]

GFI LanGuard Network Security Scanner 9.0 Beta

http://gratis.portalprogramas.com/Firewall-Commander.html [consulta 14 de diciembre de 2011]

http://www.buenastareas.com/ensayos/Tesis-Diseno-Plan-De-Seguridad-Informati ca/692955.html [consulta 03 de diciembre de 2010]

http://www.sabersinfin.com/index.php?option=com_content&task=view&id=181&Ite mid=89 [consulta 03 de diciembre de 2010]

http://www.segu-info.com.ar/tesis/ [consulta 03 de diciembre de 2010]

http://www.monografias.com/trabajos12/fichagr/fichagr.shtml [consulta 10 de mayo de 2011]

http://www.arcert.gov.ar/politica/PSI_Modelo-v1_200507.pdf [consulta 10 de mayo de 2011]

http://www.ifex.org/campaigns/2011/03/09/ejemplo_evaluacion_de_riesgos.pdf [consulta 12 de mayo de 2011]

http://www.ccee.edu.uy/ensenian/catcomp/material/Inform_%20II/riesgoinf8.pdf [consulta 13 de mayo de 2011]

http://jmpovedar.files.wordpress.com/2011/03/mc3b3dulo-4.pdf [consulta 19 de mayo de 2011]

http://www.csi.map.es/csi/pg5m20.htm [consulta 20 de mayo de 2011]

http://www.pmde.gob.pe/archivos/MANUAL_DE_POLITICAS_DE_SEGURIDAD-PMDE_13-07-2009.pdf [consulta 20 de mayo de 2011]