CAPITULO 2
ANÁLISIS PERTINENTE PARA LA REALIZACIÓN DE UN ESTUDIO DE RIESGOS Y VULNERABILIDADES

2.1 INTRODUCCIÓN

Hoy en día, los peligros al navegar por la red se incrementan por el desconocimiento o falta de prevención y no tomamos las medidas preventivas adecuadas, pese a que diariamente escuchamos alguna referencia sobre los riesgos existentes, las vulnerabilidades a las que se haya expuesta la información, como la proliferación y difusión de virus y gusanos, ataques de negación de servicio o robo de información personal y confidencial.

Sin embargo, una organización que trabaje con cualquier tipo de recurso informático, agrupaciones con negocios no relacionados directamente con las nuevas tecnologías y hasta grandes estructuras de ámbito internacional, deben estar preocupados por su seguridad y no es para menos; el número de amenazas a la información y a la comunicación crece casi exponencialmente año tras año, alcanzando niveles inimaginables. Estos riesgos llevan a que muchas personas desarrollen documentos y directrices que orientan en el uso adecuado de estas destrezas tecnológicas y recomendaciones para obtener el mayor provecho de estas ventajas, y evitar el uso indebido de la mismas, convirtiendo a la seguridad en algo complejo, no tanto desde un punto de vista técnico sino más bien desde un punto de vista organizativo ya que anteriormente la preocupación se centraba; sobre los aspectos técnicos de la seguridad, como por ejemplo: la implantación de un cortafuegos, que acabaría con todos los problemas y se elegía

el más caro aunque después nadie supiera implantar en él una política correcta ni detectar sus posibles vulnerabilidades.

Por fortuna, las cosas han empezado a cambiar, hoy en día la seguridad va más allá de lo que pueda ser un firewall, un sistema de autenticación o una red de sensores de detección de intrusos o el uso de firmas digitales; ya se contemplan aspectos que hasta hace poco se reservaban a entornos altamente cerrados, como bancos u organizaciones militares, y se ha concedido gran relevancia a las estrategias de seguridad preventiva en todos los ámbitos, llegando a una conclusión: que sin una política de seguridad correctamente implantada en cualquier dependencia no servirían de mucha ayuda controlar los acceso físicos y lógicos a la misma.

Algo que sin duda ha contribuido a todo esto es la aparición de normativas y estándares de seguridad, de ámbito tanto nacional como internacional y su aplicación en diversas áreas y organismos proporcionando como resultado el uso correcto en el ámbito de seguridad a nivel de detección de riesgos y vulnerabilidades ; por ello, en el transcurso de este análisis se utilizará como una guía básica el **[UNE-ISO/IEC 17799, 2004]**, para tener un conocimiento más claro acerca de los requisitos indispensables para proteger y gestionar la seguridad de los sistemas de información dentro de la cualquier organización. Cabe señalar que las políticas por sí solas no constituyen una garantía para la seguridad de la organización, ellas deben responder a intereses y necesidades organizacionales, basadas en la visión que cada institución posee, orientando a su personal hacia una mejor administración de los recursos informáticos, ayudando a reconocer los mecanismos de seguridad informática que en la actualidad se presentan para contravenir todos los riesgos que puede presentar una estrategia mal implantada.

Muchas veces, la terminología relacionada con el análisis de riesgos y vulnerabilidades resulta difícil de comprender, un término de fácil identificación puede ser interpretado de formas distintas por diferentes personas. Por estos motivos, es importante comprender los conceptos y definiciones que en este capítulo se abordan, para ello nos hemos dado a la tarea de realizar un análisis bibliográfico detallado y resumir lo referente a estos términos.

Antes de comenzar, creemos muy importante entender de forma general que es la Seguridad Física y que es Seguridad Lógica ya que todo nuestro estudio y análisis va a recaer sobre alguna de estas dos terminologías que es como podemos dividir la Seguridad Informática.

2.2 SEGURIDAD FÍSICA

La seguridad física es uno de los aspectos más olvidados a la hora del diseño de un sistema informático dentro de una organización, por ejemplo, detectar a un atacante en el momento que intenta acceder físicamente a una sala de operaciones de la misma.

Por ello, la Seguridad Física, se refiere a los controles y mecanismos de seguridad implementados para proteger el hardware y medios de almacenamiento de datos, prevenir las posibles amenazas y riesgos físicos de los recursos y la información confidencial, suministrando protección ante accesos no autorizados, daños e interferencias a las instalaciones de cualquier organización.

2.3 SEGURIDAD LÓGICA

El bien más importante que posee una organización, es la información, por lo tanto deben existir técnicas que la aseguren, más allá de la seguridad física que se establezca sobre los equipos en los cuales se almacena. Estas técnicas las brinda la seguridad lógica y consiste en la aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo, protegiendo la información en su propio medio mediante uso de mecanismos de seguridad lógicos. Esto lleva a aplicar un pequeño adagio, "lo que no está permitido debe estar prohibido", esto es lo que en realidad debe cumplir la seguridad lógica.

2.4 DEFINICIÓN DE BIEN

Al realizar un estudio de riesgos y vulnerabilidades que es nuestro objetivo en esta investigación, se deben identificar los bienes informáticos de la organización a partir de debates, consultas a especialistas, entrevistas a usuarios y administrativos etc. Los bienes se definen como cualquier elemento que represente un valor para la organización. Esto incluye bienes intangibles como la imagen y reputación de la organización y bienes tangibles como la infraestructura física y la información digital. Pero para entender mejor que es un bien y un bien informático analizaremos su definición y conceptos.

Según define la **[REAL ACADEMIA ESPAÑOLA, 2006],** "(Del lat. *bene*, bien).

1. m. Aquello que en sí mismo tiene el complemento de la perfección en su propio género, o lo que es objeto de la voluntad, la cual ni se mueve ni puede moverse sino por el bien**,** sea verdadero o aprehendido falsamente como tal.

2. m. Utilidad, beneficio. *El bien de la patria*

3. m. Patrimonio, hacienda, caudal. U. m. en pl.

4. m. *Fil.* En la teoría de los valores, la realidad que posee un valor positivo y por ello es estimable.

5. m. ant. Caudal o hacienda.

6. m. pl. *Der.* Cosas materiales o inmateriales en cuanto a objetos de derecho.

7. adv.U. en sent. ponder. Antepuesto a un adjetivo o adverbio, muy. U. en sent. ponderativo. *Bien tarde Bien rico Bien malo"*.

Según **[EDUCAJOB, 2006]**, "Del "bien" se habla, al menos, en cuatro sentidos diferentes:
La expresión "el bien" se ha utilizado como si designara alguna realidad o algún valor. Cuando tal realidad o valor son considerados absolutos, se habla del Sumo Bien.

- "Bien" se ha usado asimismo para designar alguna cosa valiosa, como cuando se habla de "un bien".
- "Bien" se ha usado también para indicar que algo es como es debido.

- Muchas veces “el Bien” equivale a “la bondad” cuando con esta última palabra se expresa abstractamente toda cualidad buena o cuando se trata de indicar abstractamente que algo es como debe ser”.

“La palabra bien es aplicable en general a cualquiera cosa que puede constituir riqueza o fortuna. Esta palabra hace relación al mismo tiempo a la palabra *cosas* que constituye el segundo objeto de la jurisprudencia, según la cual sus principios y reglas se refiere a las personas, a las cosas y a las acciones”. **[LEXJURIS, 2006]**

2.4.1 CONCEPTO DE BIEN

De todas las cosas que existen, hay algunas que pueden ser objeto de apropiación, es decir que pueden ser propiedad de alguien, por ejemplo un mueble, pudiendo ser éste un libro, mercancías, etc.; o bien, un inmueble, como un terreno, un edificio, todas aquellas cosas cuya propiedad pueda ser adquirida por alguien, ya sea el poder público o particular, reciben el nombre de bien o bienes.

[MORA, 2002], expresa que “'el bien' -también con mayúscula: 'el Bien'— como si esta expresión designara alguna realidad o algún valor. Cuando tal realidad o valor son considerados absolutos, se habla del Sumo Bien, *summum bonum*. 'Bien' es usado asimismo para designar alguna cosa valiosa, como cuando se habla de «un bien» o de 'bienes'. Se usa asimismo 'bien' para indicar que algo es como es debido”.

Como conclusión mencionamos que un Bien, es todo aquello que puede ser objeto de apropiación y también puede ser considerado como una cosa valiosa, utilizado para satisfacer alguna necesidad o para producir beneficios de carácter patrimonial o personal.

2.4.1.2 CONCEPTO DE BIENES INFORMÁTICOS

De acuerdo con **[MOREA,1997]**, "Bienes Informáticos son todos aquellos elementos que forman el sistema (ordenador) en cuanto al hardware, ya sea la unidad central de proceso o sus periféricos, así como todos los equipos que tienen una relación directa de uso con respecto a ellos y que, en conjunto, conforman el soporte físico del elemento informático. Asimismo, se consideran bienes informáticos los bienes inmateriales que proporcionan las órdenes, datos, procedimientos e instrucciones, en el tratamiento automático de la información y que, en su conjunto, conforman el soporte lógico del elemento informático".

Resumiendo lo expresado por **[PÉREZ, 2006]**, existe un consenso respecto al Bien Informático por su doble aspecto material e inmaterial. Los bienes materiales están representados por el hardware y los equipos periféricos, y los bienes inmateriales son los relativos a los datos e informaciones automatizados sobre la persona, incluidas imágenes, voz y sonido, ellos pueden amenazar o vulnerar los derechos de la persona, particularmente aquellos sensibles a su privacidad e intimidad.

2.5 DEFINICIÓN DE RIESGO

De acuerdo a **[ENCARTA, 2006],** riesgo "(Del it. risico o rischio, y este del ár. clás. rizq, lo que depara la providencia). m. Contingencia o proximidad de un

daño. || 2. Cada una de las contingencias que pueden ser objeto de un contrato de seguro. || a ~ y ventura. loc. adv. Dicho de acometer una empresa o de celebrar un contrato: Sometiéndose a influjo de suerte o evento, sin poder reclamar por la acción de estos. || correr ~ algo. fr. Estar expuesto a perderse o a no verificarse. □ V. grupo de ~, población de ~".

Según la **[UACAM, 2006],** riesgo es "aquel elemento del medio físico y biológico nocivo para el hombre y causado por fuerzas ajenas a él".

De acuerdo a **[BELMAR, 2006]**, riesgo es "la probabilidad que un peligro (causa inminente de pérdida), existente en una actividad determinada durante un periodo definido, ocasione un incidente con consecuencias factibles de ser estimadas".

Para la **[REAL ACADEMIA ESPAÑOLA, 2006]**, riesgo es "(Del it. *risico* o *rischio,* y este del ár. clás. *rizq*, lo que depara la providencia). **1.** m. Contingencia o proximidad de un daño. **2.** m. Cada una de las contingencias que pueden ser objeto de un contrato de seguro. **a** ~ **y ventura. 1.** loc. adv. Dicho de acometer una empresa o de celebrar un contrato: Sometiéndose a influjo de suerte o evento, sin poder reclamar por la acción de estos. **correr** ~ algo.**1.** fr. Estar expuesto a perderse o a no verificarse".

2.5.1 CONCEPTO DE RIESGO

En la dirección electrónica de **[CANCELADO, 2006]**, al respecto nos indica que, "el riesgo es una condición del mundo real en el cual hay una exposición a la adversidad, conformada por una combinación de circunstancias del entorno, donde hay posibilidad de perdidas". Valorándose al riesgo como un impacto, amenaza, vulnerabilidad y probabilidad.

De acuerdo a **[BUADES, 1999]**, "El riesgo se halla de forma implícita asociado a toda actividad:

- Todo suceso se ve marcado por las acciones del pasado, ¿Se puede, por tanto, actuar ahora para crear oportunidades en el futuro?
- El riesgo acompaña a todo cambio.
- El riesgo implica elección e incertidumbre".

2.5.2 DEFINICIÓN DE RIESGO INFORMÁTICO

Según **[WIKIPEDIA, 2006],** riesgo es "la posibilidad de que se produzca un impacto determinado en un Activo, en un Dominio o en toda la Organización".

Según **[Microsoft TechNet, 2006]**, "Un riesgo es la posibilidad de que un agente amenazante se aproveche de una vulnerabilidad. Es el potencial de pérdida o la probabilidad de que una amenaza se aproveche de una vulnerabilidad"

2.5.3 CONCEPTO DE RIESGO INFORMÁTICO

[JIMÉNEZ, 2006], expresa que riesgo informático es "La Proximidad o posibilidad de un daño, peligro, etc. Cada uno de los imprevistos, hechos desafortunados, etc., que puede cubrir un seguro".

En la dirección Web de **[PELÁEZ, 2006]**, nos explica que riesgo es la "probabilidad de que una AMENAZA se materialice sobre una VULNERABILIDAD del Sistema de Información causando un IMPACTO en la entidad".

Aludiendo a lo expresado, podemos decir que riesgo informático es la declaración intencionada de hacer un daño, donde existe la posibilidad de que cualquier amenaza ya sea física o lógica pueda materializarse.

2.6 ¿QUÉ ES UNA AMENAZA?

Una amenaza es considerada como un evento, que puede desencadenar un incidente y causar daño, cuya ocurrencia es peligrosa para las personas, propiedades, instalaciones y ambiente.

2.6.1 DEFINICIÓN DE AMENAZA

[ENCARTA, 2006], menciona que "amenaza (Del lat. vulg. mĭnacia, y este del lat. mĭna). f. Acción de amenazar. || 2. Dicho o hecho con que se amenaza. || 3. Der. Delito consistente en intimidar a alguien con el anuncio de la provocación de un mal grave para él o su familia".

La amenaza esta "definida como la probabilidad de ocurrencia de un evento potencialmente desastroso durante cierto período de tiempo en un sitio dado". **[UACAM, 2006**].

Según **[WORDREFERENCE, 2005],** amenaza es: "1 f. Dicho o hecho con que se amenaza. 2. Anuncio de un mal o peligro".

Para la **[REAL ACADEMIA ESPAÑOLA, 2006]**, amenaza "(Del lat. vulg. *mĭnacia,* y este del lat. *mĭna*).
1. f. Acción de amenazar.

2. f. Dicho o hecho con que se amenaza.

3. f. pl. *Der.* Delito consistente en intimidar a alguien con el anuncio de la provocación de un mal grave para él o su familia".

Según el diccionario **[OCÉANO PRÁCTICO, 2006]**, amenaza es: "Dar a entender con actos o palabras que se quiere hacer algún mal a otro".

2.6.2 ¿QUÉ ES UNA AMENAZA INFORMÁTICA?

Son aquellos sucesos que pueden liberar un accidente en la organización, produciendo daños materiales o pérdidas inmateriales en los bienes informáticos.

2.6.3 DEFINICIÓN DE AMENAZA INFORMÁTICA

La página Web de **[Tuarroba, 2006]**, define que amenaza informática es un "posible peligro del sistema. Puede ser una persona (cracker), un programa (virus, caballo de Troya, etc.), o un suceso natural o de otra índole (fuego, inundación, etc.). Representan los posibles atacantes o factores que aprovechan las debilidades del sistema".

Para **[WIKIPEDIA, 2006],** amenaza informática es considerada como un "evento que pueden desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos".

2.6.4 CONCEPTO DE AMENAZA INFORMÁTICA

Se entiende por amenaza una condición del entorno del sistema de información que, dada una oportunidad, podría dar lugar a que se produjese una violación de la seguridad (confidencialidad, integridad, disponibilidad o uso legítimo). La política de seguridad y el análisis de riesgos deben identificar las amenazas que han de ser contrarrestadas, y especificar los mecanismos de seguridad necesarios para hacerlo. Un ataque no es más que la realización de una amenaza y debe ser evitado por la implementación de las políticas. **[BALUJA, 2000].**

Según **[HOWARD, 2006],** "Una amenaza informática es una persona, un lugar o un elemento que puede tener acceso a los recursos y dañarlos".

[POLK, 2006], expresa que "una amenaza es cualquier peligro potencial para la información o los sistemas".

2.6.5 TIPOS DE AMENAZAS INFORMÁTICAS

Básicamente hay tres aspectos que se ven amenazados: el hardware (el sistema), el software (programas de usuarios, aplicaciones, bases de datos, sistemas operativos, etc.), los datos; dependiendo de las fuentes de amenazas, ellas se dividen en amenazas físicas y lógicas.

2.6.5.1 AMENAZAS FÍSICAS

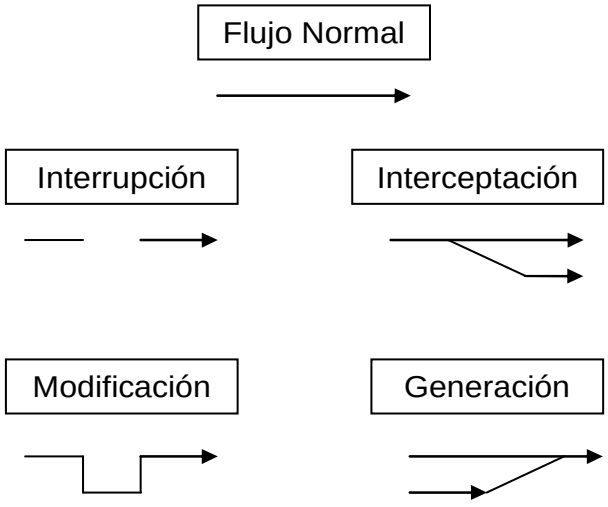
Son las que ponen en peligro los componentes físicos del sistema. En ellas podemos distinguir por un lado los desastres naturales y por otro las condiciones medioambientales.

Entre ellas podemos citar algunas:

- Inundaciones (intensas lluvias, riadas, etc.).
- Inundaciones internas.
- Fuegos.
- Humedad.
- Presencia de polvo.
- Rayos.
- Interferencias electromagnéticas.
- Terremotos.
- Temperatura.

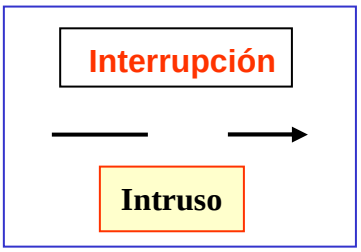
2.6.5.2 AMENAZAS LÓGICAS

Estas se deben a fenómenos de: interrupción, interceptación, modificación, generación; causados a los sistemas de información por personas u accidentes informáticos en una forma voluntaria o involuntaria. Como podemos apreciar en la siguiente figura:



CAP2 Fig. 2.6.5.2 Amenazas Lógicas a los Sistemas Informáticos

Interrupción

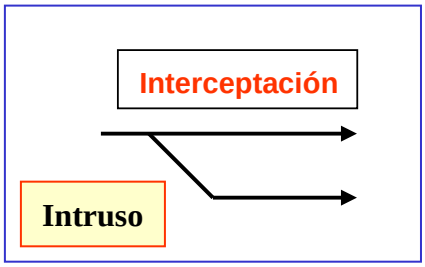


Interrupción mediante algún método al funcionamiento del sistema, puede ser intencional o accidental, se daña, pierde o deja de funcionar un punto del sistema su detección suele ser inmediata.

Ejemplos:

- Destrucción del hardware.
- Borrado de programas, datos.
- Fallos en el sistema operativo.
- Saturar la memoria o el máximo de procesos en el sistema operativo.
- Destruir algún dispositivo hardware

Interceptación

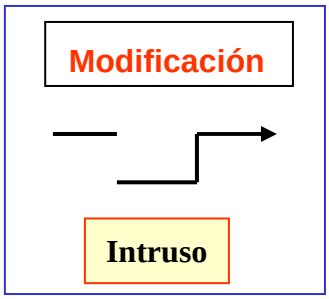


Acceso a la información por parte de personas no autorizadas. Uso de privilegios no adquiridos, su detección es difícil, no deja huellas.

Ejemplos:

- Copias ilícitas de programas
- Escucha en línea de datos

Modificación

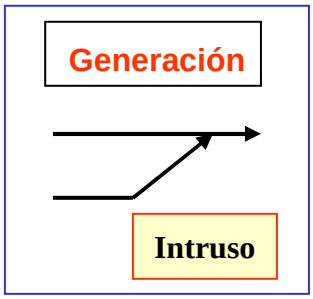


Se trata no sólo de acceder a una parte del sistema a la que no se tiene autorización, sino de cambiar, en todo o en parte, su contenido o modo de funcionamiento.

Ejemplos:

- Modificación de bases de datos.
- Modificación de elementos del HW.
- Cambiar líneas de código en un programa.
- Cambiar datos en una transferencia bancaria.
- Rotura de Contraseñas.

Generación



Se refiere a la posibilidad de añadir información o programas no autorizados en el sistema, creando nuevos objetos, también son de difícil detección, aquí podemos citar el origen de los delitos de la información

Ejemplos:

- Añadir transacciones en red.
- Añadir registros en base de datos.
- Añadir campos y registros en una base de datos.
- Añadir códigos en un programa (virus).
- Introducir mensajes no autorizados en una línea de datos.
- Herramientas de Hacking y Cracking que se ofrecen como FREEWARE.

Como puede observarse, la inseguridad lógica es muy grande, debido a la variedad de los medios de amenazas, pero otra amenaza que hay que tomar en consideración y que para muchas personas pasan desapercibidas son las amenazas involuntarias

2.6.5.3 AMENAZAS INVOLUNTARIAS.

Son aquellas que pueden ser físicas o lógicas y están relacionadas con el uso descuidado del equipo por falta de entrenamiento o de concientización sobre la seguridad. Entre las más comunes podemos mencionar:

- Borrar sin querer parte de la información.
- Dejar sin protección determinados ficheros básicos del sistema.
- Dejar pegado a la pantalla un post-it con nuestro password u olvidarnos de salir del sistema.
- Entrando al edificio o accediendo físicamente a la información del ordenador.
- Errores, omisiones o accidentes

Como podemos ver, las intervenciones maliciosas por manipulaciones humanas o no, son imprevisibles y de un resultado incierto; personalmente comentamos que en la actualidad no existe límite alguno a la hora de tener una amenaza en los recursos informáticos, pues uno de los cambios más sorprendentes en el mundo es la rapidez de las interconexiones. Esto ha causado que la mayoría de las personas hagan un uso masivo del Internet, facilitando que todo tipo de información viaje a cualquier lugar del mundo y se encuentre disponible en la red a la hora que deseemos, lo cual, lógicamente, ha traído consigo la aparición de los denominados “virus informáticos” que constituyen uno de los mayores riesgos de seguridad a nivel mundial para los sistemas y recursos de información, estos pueden afectar en diferentes formas desde un simple usuario hogareño que utiliza su máquina para trabajar y conectarse a Internet o a una gran empresa o institución en general que manejen sistemas informáticos muy importantes y deben mantener bajo constante vigilancia estos riesgos para evitar pérdidas en

sus bienes informáticos, motivo por el cual es de vital importancia conocer algunos aspectos básicos de este tipo de amenazas que día tras día nos agobian.

2.7 ¿QUÉ ES UN VIRUS?

Según **[QUINTERO, 2002]**, virus "Es un pequeño programa escrito intencionalmente para instalarse en la computadora de un usuario sin el conocimiento o el permiso de este. Decimos que es un programa parásito porque el programa ataca a los archivos o sectores de "booteo" y se replica a sí mismo para continuar su esparcimiento".

De acuerdo a **[ADELAFLOR, 2006]**, virus es "Un archivo pequeño que actúa sobre tu ordenador sin tu consentimiento con el fin de hacer que funcione mal o de manera extraña, o con otros propósitos todos ellos no deseados por ti".

"El virus informático es un programa elaborado accidental o intencionadamente, que se introduce y se transmite a través de diskettes o de la red telefónica de comunicación entre ordenadores, causando diversos tipos de daños a los sistemas computarizados"**. [JIMÉNEZ, 2006].**

2.7.1 ¿CÓMO NACIERON LOS VIRUS?

Hacia finales de los años 60, Douglas McIlory, Víctor Vysottsky y Robert Morris, idearon un juego al que llamaron Core War (Guerra en lo Central, aludiendo a la memoria de la computadora), que se convirtió en el pasatiempo de algunos de los programadores de los laboratorios Bell de AT&T.

El juego consistía en que dos jugadores escribieran cada uno un programa llamado organismo, cuyo hábitat fuera la memoria de la computadora. A partir de una señal, cada programa intentaba forzar al otro a efectuar una instrucción inválida, ganando el primero que lo consiguiera.

Al término del juego, se borraba de la memoria todo rastro de la batalla, ya que estas actividades eran severamente sancionadas por los jefes por ser un gran riesgo dejar un organismo suelto que pudiera acabar con las aplicaciones del día siguiente. De esta manera surgieron los programas destinados a dañar en la escena de la computación.

Actualmente, los virus son producidos en cantidades extraordinarias por muchísima gente alrededor del planeta. Algunos de ellos dicen hacerlo por diversión, otros quizás para probar sus habilidades. De cualquier manera, hasta se ha llegado a notar un cierto grado de competitividad entre los autores de estos programas.

2.7.2 TIPOS DE VIRUS

Los virus se clasifican por el modo en que actúan infectando la computadora:

- Programa: Infectan archivos ejecutables tales como .com / .exe / .ovl / .drv / .sys / .bin.
- Boot: Infectan los sectores Boot Record, Master Boot, FAT y la Tabla de Partición.
- Múltiples: Infectan programas y sectores de "booteo".
- Bios: Atacan al Bios para desde allí reescribir los discos duros.

- Hoax: Se distribuyen por e-mail y la única forma de eliminarlos es el uso del sentido común.

2.7.3 CARACTERÍSTICAS DE LOS VIRUS.

El virus es un pequeño software (cuanto más pequeño más fácil de esparcir y más difícil de detectar), que permanece inactivo hasta que un hecho externo hace que el programa sea ejecutado o el sector de "booteo" sea leído. De esa forma el programa del virus es activado y se carga en la memoria de la computadora, desde donde puede esperar un evento que dispare su sistema de destrucción o se replique a sí mismo.

Además de reproducirse, algunos virus informáticos tienen algo en común: una rutina dañina, que el virus descarga como una bomba, mientras que las descargas pueden ser simples mensajes o imágenes, éstas también pueden borrar archivos, reformatear el disco duro o causar otro tipo de daño. Si el virus no contiene una rutina dañina, aún puede causar problemas, como tomar espacio libre del disco y de la memoria, y también disminuir el rendimiento de la computadora.

Los más comunes son los residentes en la memoria que pueden replicarse fácilmente en los programas del sector de "booteo". Los menos comunes son los no-residentes que no permanecen en la memoria después que el programa-huésped es cerrado.

2.8 QUÉ ES VULNERABILIDAD

Vulnerabilidad de un bien, es la posibilidad de que una amenaza se materialice sobre él, conociendo los puntos de exposición de los sistemas de información que puedan generar en un riesgo para la información del mismo.

2.8.1 DEFINICIÓN DE VULNERABILIDAD INFORMÁTICA

Para **[Tuarroba, 2006]**, Vulnerabilidad Informática es el "punto o aspecto del sistema que es susceptible de ser atacado o de dañar la seguridad del mismo. Representan las debilidades o aspectos falibles o atacables en el sistema informático".

[WKIPEDIA, 2006], Vulnerabilidad Informática es "posibilidad de ocurrencia de la materialización de una amenaza sobre un Bien".

2.8.2 CONCEPTO DE VULNERABILIDAD INFORMÁTICA

"Una vulnerabilidad es un software, hardware o deficiencia de procedimiento que podría darle a un atacante o agente amenazante la oportunidad de introducirse en un equipo o red, y tener acceso a recursos dentro del entorno sin autorización". **[POLK, 2006].**

Según **[ADELAFLOR, 2006],** vulnerabilidad informática es "un problema o fallo que se ha descubierto en un programa y que aprovechan los virus".

También podemos mencionar que una vulnerabilidad es el punto donde un bien informático se vuelve susceptible a cualquier amenaza y por ende puede estar

latente un riesgo, por ello, es considerada como una debilidad para cualquier recurso o sistema de información en sentido físico y lógico, teniendo en cuenta que una vulnerabilidad por si misma no produce daños sino, es un condicionante para que una amenaza afecte a un bien informático.

2.8.3 TIPOS DE VULNERABILIDAD

La seguridad es la facultad de estar a protegido de algún riesgo o amenaza. Desde este punto de vista la seguridad total es muy difícil de logra, puesto que implicaría describir todos los riesgos y amenazas a que puede verse sometido un recursos informático. No se puede hablar de un sistema informático totalmente seguro, sino más bien de uno en el que no se conocen tipos de ataques que puedan vulnerarlo, debido a que se han establecido medidas contra ellos. Entre tipos de vulnerabilidad más importantes podemos señalar los siguientes:

2.8.3.1 VULNERABILIDAD FÍSICA:

Se refiere al grado en que el sistema puede verse afectado por desastres naturales o ambientales que pueden dañar el sistema, tales como el fuego, inundaciones, rayos, terremotos, o quizás más comúnmente, fallos eléctricos o picos de potencia.

También el polvo, la humedad o la temperatura excesiva son aspectos a tener en cuenta. Otro aspecto es la posibilidad de entrar o acceder físicamente al sistema para robar o dañar los discos, cintas, listados de impresora, etc.

Ejemplos:

- Puertas sin cerrojo.
- Acceso no protegido a las instalaciones informáticas.

- Sistemas contra incendios insuficientes.
- Diseño deficiente de edificios.
- Construcción deficiente de edificios.
- Materiales inflamables empleados en la construcción.
- Materiales inflamables empleados en el acabado.
- Ventanas sin cerrojo.
- Paredes que se pueden asaltar físicamente.
- Paredes interiores que no sellan la sala por completo tanto en el techo como en el suelo.
- Instalación situada sobre una línea de error.
- Instalación situada en una zona de inundaciones.
- Instalación situada en un área de avalanchas.

2.8.3.2 VULNERABILIDAD LÓGICA:

La conexión de los ordenadores a redes supone sin duda un enorme incremento de la vulnerabilidad del sistema. Aumenta enormemente la escala del riesgo al que está sometido, al aumentar la cantidad de gente que puede tener acceso al mismo o intentar tenerlo. También se añade a este riesgo de intercepción de las comunicaciones:

donde se puede introducir al sistema a través de la red, interceptando la información que es transmitida desde o hacia el sistema. Desde el punto de vista del hardware, ciertos tipos de dispositivos pueden ser más vulnerables que otros, algunos sistemas requieren la posesión de algún tipo de herramienta o tarjeta para poder acceder a los mismos. Estos fallos o debilidades del software hacen más fácil acceder a los sistemas y lo hacen menos fiables.

Ejemplos:

- Software antivirus obsoleto.
- Aplicaciones escritas deficientemente.
- Vulnerabilidades de código como desbordamientos de búfer.
- Vulnerabilidades colocadas deliberadamente.
- Puertas traseras del proveedor para la administración o la recuperación del sistema.
- Programas espía como aplicaciones de captura de teclado.
- Troyanos.
- Errores de configuración.
- Sistemas no protegidos.
- Sistemas no auditados.
- Sistemas no supervisados.
- Protocolos de red sin cifrar.
- Conexiones a varias redes.
- Sin filtrado entre segmentos de red.
- Sistemas configurados incorrectamente.
- Protocolos de administración permitidos en interfaces públicas.
- Carencia o insuficiencia de los mecanismos de identificación y autenticación.
- Gestión de contraseñas: comparición, pérdida, adivinación.
- Problemas del S.O.: agujeros.
- Acceso físico no controlado:
- PC desprotegido.
- módems abiertos.
- Cables expuestos.
- monitores, impresoras expuestos.

- Exposición del tráfico interno:

  origen, destino, volumen o frecuencia

2.8.3.3 VULNERABILIDAD HUMANA

Las personas que administran y utilizan el sistema representan la mayor vulnerabilidad. Toda la seguridad del sistema descansa sobre el administrador del mismo que tiene acceso al máximo nivel y sin restricciones a estos recursos. Los usuarios del sistema también son considerados como un gran riesgo, ellos pueden acceder al mismo, tanto físicamente como mediante conexión. Existen estudios que demuestran que la mayor parte de los problemas de seguridad detectados son debidos a los usuarios.

Ejemplos:

- Preparación insuficiente para la respuesta a incidencias.
- Procedimientos definidos deficientemente en :
  - Creación de manuales.
  - Planes de recuperación de desastres insuficientes.
  - Pruebas en sistemas de producción.
  - Infracciones no comunicadas.
  - Control de cambios deficientes.
  - Credenciales robadas.

Como resumen a todos los conceptos y definiciones que mencionamos anteriormente podemos decir que la relación entre amenazas, vulnerabilidades y riesgos puede ser difícil de entender al principio, pues cada amenaza y

vulnerabilidad que se identifique dentro de una organización debe ser calificada y clasificada de acuerdo a la metodología implantada para cada una de ellas.

2.9 MEDIDAS DE SEGURIDAD

Las medidas de seguridad permiten minimizar los riesgos y amenazas sobre los sistemas y recursos de información, garantizan y establecen en detalle los pasos precisos para proteger la continuidad de los procesos informáticos, su definición clara y precisa, evitará interpretaciones ambiguas por parte de los responsables de su cumplimiento

2.9.1 MEDIDAS FÍSICAS

Estas aplican mecanismos para impedir el acceso directo o físico y no autorizado a los recursos o sistemas informáticos, protegiéndolo de esta manera de desastres naturales o condiciones medioambientales adversas.

Existen tres factores fundamentales a considerar:

- El acceso físico al sistema por parte de personas no autorizadas.
- Los daños físicos por parte de agentes nocivos o contingencias.
- Las medidas de recuperación en caso de fallo.

Ejemplos:

- Archivos y documentación de reserva Detectores de movimiento.
- Rejas, detectores de humo y fuego.
- Guardias de seguridad.
- Monitorización por televisión de circuito cerrado.
- Sistemas de tarjetas de identificación.

- Sensores y alarmas.
- Cerraduras y llaves.
- Candados cifrados.
- Potencia de reserva.
- Controles biométricos de acceso.
- Extintores de incendios.
- Bloqueo de teclados.

2.9.2 MEDIDAS LÓGICAS.

Incluye las medidas de acceso a los recursos y a la información y al uso correcto de los mismos, así como a la distribución de las responsabilidades entre los usuarios. Se refiere más a la protección de la información almacenada.

Ejemplos:

- Programas de control de acceso logs y diseño para auditaría.
- Programas cortafuegos y antivirus, sistemas expertos de detección de intrusiones.
- Gestión de contraseñas.
- Tarjetas inteligentes.
- Cifrado.

2.9.3 MEDIDAS ADMINISTRATIVAS.

Las medidas administrativas son aquellas que deben ser tomadas por las personas encargadas de definir la políticas de seguridad para ponerlas en práctica, hacerla viables y vigilar su correcto funcionamiento.

Ejemplos:

- Conocimientos de seguridad y formación técnica.
- Revisiones y auditorias de seguridad.
- Separación de obligaciones.
- Control de calidad.
- Políticas y procedimientos de seguridad.
- Rotación de responsabilidades.
- Gestión y supervisión.
- Recuperación de averías y planes de contingencia.
- Administración de accesos de usuarios.
- Gestión de propietarios de datos y recursos.

En conclusión podemos expresar, que implantar una buena medida de seguridad informática es el primer paso que debemos tener en cuenta para proteger la confidencialidad, integridad, disponibilidad de la información y los recursos del sistema.

Estas medidas deben ser implantadas, incluyendo en cada una, la combinación de mecanismos lógicos, físicos, administrativo y su elección se facilitará dependiendo a los tipos de amenazas y riesgos que se presenten para poder implantar los mecanismos con eficacia, ayudando de esta manera a los responsables de la seguridad a canalizarla hacia una objetivo común que sea realista, factible y en beneficio propio de la institución en general.

2.10 POLÍTICAS DE SEGURIDAD

2.10.1 INTRODUCCIÓN

Las políticas de seguridad informática representan un tipo especial de reglas documentadas. Su incremento ha sido estimulado por la explosión de tecnologías de manejo de información, incluyendo a los teléfonos celulares, los buscapersonas y los computadores, por ello, la seguridad informática depende de la articulación eficiente de varios factores, uno de los cuales es el conjunto de políticas de seguridad informática, las cuales representan el marco normativo de mayor importancia para el establecimiento de cualquier solución de seguridad para las organizaciones.

El no administrar correctamente una política de seguridad informática denota no sólo negligencia, sino que constituye una invitación para que ocurran incidentes de seguridad que podrían dañar severamente todos los recursos de cualquier organización.

Las políticas de seguridad informática, son instrucciones que trazan una dirección predeterminada o describen la manera de manejar un problema o situación, estas ayudan a los usuarios de dichos recursos a orientarse para tomar decisiones presentes y futuras así como también son requisitos generalizados que deben ser elaborados y comunicados a los grupos de entes dentro, y en algunos casos fuera, de una organización.

En este sentido, las políticas de seguridad informática surgen como una herramienta para concientizar a las personas, sobre la importancia, la sensibilidad de la información y servicios críticos que permiten a cualquier organización crecer y mantenerse fuera de ciertos riesgos que pueden afectar la integridad de la

misma, por tal motivo establecer una política y poner en marcha constituye un alto compromiso con cualquier organismo, para establecer fallas y debilidades, y constancia para renovar y actualizar dicha política en función al ambiente que rodea las actuales organizaciones.

2.10.2 DEFINICIÓN DE POLÍTICAS DE SEGURIDAD INFORMÁTICA

Según **[AUDITORIASISTEMAS, 2004]**,"Las políticas de seguridad son las reglas y procedimientos que regulan la forma en que una organización previene, protege y maneja los riesgos de diferentes daños".

"Una política de seguridad informática es una forma de comunicarse con los usuarios, ya que las mismas establecen un canal formal de actuación del personal, en relación con los recursos y servicios informáticos de la organización". **[MONOGRAFÍAS, 2006]**

2.10.3 CONCEPTO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA

El término política de seguridad suele puntualizar como el conjunto de requisitos definidos por los responsables directos o indirectos de un sistema que indica en términos generales qué está y qué no está permitido en el área de seguridad durante la operación general de dicho sistema **[VILLALÓN, 2002]**.

Según **[TORRES, 2003],** expresa que "una política de seguridad informática es una forma de comunicarse con los usuarios, ya que las mismas establecen un

canal formal de actuación del personal, en relación con los recursos y servicios informáticos de la organización".

De acuerdo a **[CANO, 2006],** "una política de seguridad informática es una forma de comunicarse con los usuarios y los gerentes. Las PSI establecen el canal formal de actuación del personal, en relación con los recursos y servicios informáticos importantes de la organización, esto no es una descripción técnica de mecanismos de seguridad, ni una expresión legal que involucre sanciones a conductas de los empleados, es más bien una descripción de los que deseamos proteger y el por qué de ello.

Cada PSI es una invitación de la organización a cada uno de sus miembros a reconocer la información como uno de sus principales activos así como, un motor de intercambio y desarrollo en el ámbito de sus negocios. Invitación que debe concluir en una posición consciente y vigilante del personal por el uso y limitaciones de los recursos y servicios informáticos críticos de la compañía".

Por ello, podemos considerar que una política de seguridad informática no es una descripción técnica de mecanismos, ni una expresión legal que involucre sanciones a conductas de los empleados, es más bien una descripción de los que deseamos proteger y él por qué de ello, pues cada política de seguridad es una invitación a cada uno de sus miembros a reconocer la información como uno de sus principales activos así como, un motor de intercambio y desarrollo en el ámbito de sus negocios. Por tal razón, las políticas de seguridad deben concluir en una posición consciente y vigilante del personal por el uso y limitaciones de los recursos y servicios informáticos.

2.10.4 ELEMENTOS DE UNA POLÍTICA DE SEGURIDAD INFORMÁTICA

Como una política de seguridad debe orientar las decisiones que se toman en relación con la seguridad, se requiere la disposición de todos los miembros de una organización para lograr una visión conjunta de lo que se considera importante.

Las Políticas de Seguridad Informática deben considerar los siguientes elementos:

- Alcance de las políticas, incluyendo facilidades, sistemas y personal sobre la cual aplica.
- Objetivos de la política y descripción clara de los elementos involucrados en su definición.
- Responsabilidades por cada uno de los servicios y recursos informáticos aplicado a todos los niveles de la organización.
- Requerimientos mínimos para configuración de la seguridad de los sistemas que abarca el alcance de la política.
- Definición de violaciones y sanciones por no cumplir con las políticas.
- Responsabilidades de los usuarios con respecto a la información a la que tiene acceso.

Las políticas de seguridad informática, también deben ofrecer explicaciones comprensibles sobre por qué deben tomarse ciertas decisiones y explicar la importancia de los recursos. Igualmente, deberán establecer las expectativas de la organización en relación con la seguridad y especificar la autoridad responsable de aplicar los correctivos o sanciones.

Otro punto importante, es 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.

Por último, las políticas de seguridad, deben seguir un proceso de actualización periódica sujeto a los cambios organizacionales, como son: el aumento de personal, cambios en la infraestructura computacional, alta rotación de personal, desarrollo de nuevos servicios, etc.

2.10.5 ALGUNOS PARÁMETROS PARA ESTABLECER POLÍTICAS DE SEGURIDAD

- Efectuar un ejercicio de análisis de riesgos informático, a través del cual valore sus activos. Este permitirá afinar las PSI de su organización.
- Involucrar a las áreas propietarias además de los recursos o servicios, pues ellos poseen la experiencia y son fuente principal para establecer el alcance y las definiciones de violaciones a la PSI.
- Comunicar a todo el personal involucrado en el desarrollo de las PSI, los beneficios y riesgos relacionados con los recursos y bienes, y sus elementos de seguridad.
- Recordar que es necesario identificar quién tiene la autoridad para tomar decisiones, pues son ellos los interesados en salvaguardar los activos críticos de la funcionalidad de su área u organización.

- Desarrollar un proceso de monitoreo periódico de las directrices en el hacer de la organización, que permita una actualización oportuna de las mismas. **[CANO, 2006].**

2.10.6 CARACTERÍSTICAS DE UNA BUENA POLÍTICA

- Debe estar escrita en lenguaje simple, pero jurídicamente viable.
- Debe basarse en las razones que tiene la organización para proteger la información.
- Debe ser consistente con las demás políticas organizacionales
- Debe hacerse cumplir - se exige y mide el cumplimiento
- Debe tener en cuenta los aportes hechos por las personas afectadas por la política
- Debe definir el papel y responsabilidades de las personas, departamentos y organizaciones para los que aplica la política.
- Debe poder hacerse cumplir por medio de herramientas de seguridad donde sea apropiado y con sanciones donde su prevención no sea técnicamente posible.
- Debe definir claramente las áreas de responsabilidad de los dirigentes, usuarios y administradores.
- No debe violar las políticas locales, estatales
- Debe definir las consecuencias en caso de incumplimiento de la política
- Debe estar respaldada por documentos "palpables", como los estándares y procedimientos para la seguridad de la información, que se adapten a las necesidades, requerimientos jurídicos s y los cambios tecnológicos.

2.10.7 PUESTA EN MARCHA DE UNA POLÍTICA DE SEGURIDAD

La seguridad informática debe ser estudiada para que no impida el trabajo de los usuarios en lo que les es necesario y que puedan utilizar el sistema o recursos informáticos con toda confianza. Por eso, en lo referente a elaborar una política de seguridad, conviene:

- Elaborar reglas y procedimientos para cada servicio de la organización.
- Definir las acciones a emprender.
- Elegir las personas a contactar en caso de detectar una posible intrusión.
- Sensibilizar los operadores con los problemas ligados con la seguridad de los sistemas informáticos.

Los derechos de acceso de los usuarios deben ser definidos por los responsables jerárquicos y no por los administradores informáticos, los cuales tienen que conseguir que los recursos y derechos de acceso sean coherentes con la política de seguridad definida. Además, como el administrador suele ser el único en conocer perfectamente el sistema o recursos de la información, tiene que comunicar a su autoridad superior cualquier problema e información relevante que suceda sobre el aspecto de la seguridad, y eventualmente aconsejar estrategias a poner en marcha, y ser el punto de comunicación con los usuarios sobre problemas y recomendaciones que se deben realizar.

2.10.8 ¿POR QUÉ LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA GENERALMENTE NO SE LOGRAN IMPLANTAR?

Muchas veces las organizaciones realizan grandes esfuerzos para definir sus directrices de seguridad y concretarlas en documentos que orienten las acciones

de las mismas, con relativo éxito. Según algunos estudios resulta una labor ardua el convencer a las altas autoridades de la necesidad de buenas políticas y prácticas de seguridad informática.

Muchos de los inconvenientes se inician por los tecnicismos informáticos y la falta de una buena estrategia de seguridad, esto ha llevado a que muchas instituciones estén expuestas a graves problemas de seguridad, que en muchos de los casos lleva a comprometer su información sensitiva y por ende su imagen institucional.

Ante todo esto, los encargados de la seguridad deben asegurarse de que las personas entiendan la importancia de la seguridad, conozcan sus alcances y estén de acuerdo con las decisiones tomadas en relación con estos asuntos.

Para que la políticas logren abrirse espacio al interior de una organización deben integrarse a las estrategias implantadas, a su misión y visión con el propósito de que los que toman las decisiones reconozcan su importancia e incidencias en las proyecciones y utilidades de una organización, de igual forma, las políticas de seguridad informática deben ir acompañadas de una visión que promueva actividades que involucren a las personas en su diario hacer, donde se identifiquen las necesidades y acciones que materializan las políticas.

En este contexto, el entender a la organización, sus elementos culturales y comportamientos nos deben llevar a reconocer las pautas de seguridad necesaria y suficiente que aseguren confiabilidad en las operaciones y funcionalidad de cualquier entidad.

En conclusión expresamos que es importante señalar, que las políticas por sí solas no constituyen una garantía para la seguridad de la organización, éstas deben responder a los intereses y las necesidades organizacionales basadas en su misión y visión, que lleven a un esfuerzo conjunto de sus actores por administrar sus recursos, y a reconocer en los mecanismos de seguridad informática los factores que faciliten la formalización y materialización de los compromisos adquiridos con la organización.