CAPITULO 1
ASPECTOS GENERALES DE SEGURIDAD INFORMÁTICA

1.1 INTRODUCCIÓN

A finales del siglo XX, los Sistemas Informáticos han constituido las herramientas más poderosas para materializar algunos conceptos muy vitales y necesarios para cualquier organización o Institución Educativa. Consecuentemente con lo mencionado el ejercicio de nuestra profesión, no puede ser una excepción en cuanto a utilizar la Seguridad Informática como un medio para desarrollar estrategias que tributen en gran parte a disminuir las crecientes amenazas del mundo informático y de alguna forma poder tener una mejor sensación de seguridad, que dará como resultado la eficiencia y la eficacia en el uso adecuado de los sistemas y recursos de un organismo.

La Seguridad Informática debe velar por la buena utilización de los amplios recursos que la organización o institución pone en juego para disponer de un adecuado control sobre los mismos. Claro está, que para la realización de una buena propuesta de seguridad, se debe entender a la entidad en su más amplio sentido, ya que una Universidad, un Ministerio o un Hospital son instituciones que deben funcionar y prestar servicios en su más alto nivel.

Todas estas deben brindar un ambiente seguro, no por el hecho que involucre sanciones a conductas, sino más bien por encaminarnos a la forma correcta de lo que deseamos proteger y el por qué de ello. Por tanto, la intención de nuestra propuesta de Seguridad Informática pretende brindar una mejor visión acerca de las múltiples vulnerabilidades frente a los riesgos que pueden atentar contra la confidencialidad, la integridad y la disponibilidad de los recursos informáticos, la cual se elabora en base a la identificación de los riesgos y amenazas tanto internas como externas de toda la Infraestructura Informática de la Institución; ya que gran parte de las personas no prestan una especial atención a estos temas , pero parte de la solución de esta presente propuesta, recae en nosotros como usuarios al crear conciencia de que utilizar el computador de cierta manera o

incumplir las políticas y disposiciones pueden afectar a un conglomerado de personas.

El trabajo propuesto está estructurado de la siguiente manera: En el Capítulo I del documento se presentan los aspectos generales de la seguridad, conceptos de Seguridad Informática , y demás elementos que engloban dicho término que es muy usado y conocido en la actualidad, lo que permite tener un conocimiento científico para fundamentar adecuadamente la propuesta de investigación.

En el Capítulo II abordaremos un estudio de políticas de seguridad, amenazas, riesgos y vulnerabilidades a las que se hayan expuestos los recursos informáticos.

En el Capítulo III se realiza un trabajo de campo efectuado en la Universidad de Pinar del Río, contiene el levantamiento de información que permite tener un amplio conocimiento del objeto de estudio. Se presenta el Diseño de la Propuesta de Perfeccionamiento, la misma que contiene los resultados que serán entregados a la Universidad de Pinar del Río como un aporte del grupo investigador.

Por último finalizaremos esta investigación con la recopilación bibliográfica que recoge aquellas referencias más utilizadas para el desarrollo de nuestro trabajo, también están presentes las Conclusiones, Recomendaciones y Anexos que contienen información referente a normas y reglamentos.

1.2 DESCRIPCIÓN DE LOS TÉRMINOS ASOCIADOS AL TEMA

En el presente capítulo haremos referencia a los principales términos y a las definiciones más utilizadas en la actualidad en lo que respecta a Seguridad Informática.

1.2.1 SEGURIDAD

La Seguridad debe ser interpretada como un estado personal que nos permite percibir que nos movemos en un espacio libre de riesgos reales o potenciales, la ausencia o la falta de esta puede originar diversos problemas y daños.
Por ello debemos considerar que "seguridad" está asociado a la certeza, falta de riesgo o contingencia, ya que no siendo posible la certeza absoluta, el elemento de riesgo está siempre presente, independiente de las medidas que tomemos, por lo que debemos hablar de que nunca existirá un nivel de Seguridad total.

1.2.1.1 EVOLUCIÓN DEL TÉRMINO SEGURIDAD

Resumiendo lo expuesto por **[MANUNTA, 2006]**, "Seguridad es una necesidad básica, estando interesada con la preservación de la vida y las posesiones, es tan antigua como la vida sus indicios se encuentran plasmados desde el inicio de la escritura. La evidencia escrita más temprana de la seguridad se encuentra en códigos legales, tales como el Sumerio (3.000ac) o el de Hammurabi (2.000ac). Más tarde, aparece en obras, generalmente refiriéndose al arte de la guerra y gobierno. La Biblia, Homero, Sun Tzu, Cicerón, Virgilio, Cesar, Frontino, Suetonio, Joseph, Vegetio, son ejemplos relevantes de obras de autores donde ciertas evidencias de temas y principios de seguridad son halladas".

Otra evidencia puede ser encontrada en la arqueología y la antropología. Por ejemplo, podemos razonablemente asumir que la cultura y habilidades de seguridad son reconocibles en actuales culturas primitivas que son muy cercanas a las de nuestros ancestros. Desde su nacimiento, las personas son instruidas, vía tradición y entrenamiento, y/o vía imitación, en las habilidades para la seguridad. Los bebés son instruidos en no llorar en las proximidades de un enemigo, y son entrenados desde su infancia en reconocer y evitar peligros, a dar alarma, y a esconderse y refugiarse en caso de necesidad, los pueblos primitivos estaban ciertamente en alerta sobre los peligros, y antes de que métodos defensivos emergieran, sólo podían reaccionar como los animales, intentando

tanto evitar las amenazas más temidas, o eliminado su causa, dentro del bien conocido patrón de “luchar o huir (flight or fight)”domesticaron animales para obtener alarma y soporte, para reaccionar organizadamente como equipos, de acuerdo con bien planeadas y ensayadas tácticas, cuando el combate era considerado inevitable, o cuando la potencial pérdida fuera letal.

La evidencia de medidas de seguridad acompaña cada descubrimiento arqueológico. Cerraduras, puertas fuertes, ventanas selladas, trampas, cajas fuertes, sistemas de alarma, barreras físicas y escudos son conocidos y usados desde el principio de la civilización. La más antigua cerradura conocida data de 4.000ac, y fue encontrada en el palacio de Sargon, Khorsabad, cerca de Nineveh. En el 1.000ac, el dios egipcio Anubis fue representado con una llave en su mano derecha, etc.

De acuerdo con la evidencia anterior, no existe duda de que las nociones de alertar, evitar, detectar, alarmar y reaccionar son tan antiguos como la vida misma, siendo una parte esencial de la pugna diaria por la vida, y están fundados en el instinto básico de supervivencia.

La seguridad ha seguido un patrón de evolución dentro de la organización social, desde la familia al clan/banda, tribu, reino y estado. Muy pronto fue claro que los grupos eran menos vulnerables a las amenazas que las personas individuales: proveían una disuasión/intimidación por su mero número; hicieron posible la organización de centinelas y guardias, y facilitaron tácticas básicas defensivas. La institución de la familia y el descubrimiento de técnicas básicas de agricultura aportaron una importante limitación del fundamental principio de escape: la exigencia de defender la familia, la residencia y los medios de supervivencia (niños, reservas de comida, cosechas y porciones vitales de territorio) de animales y enemigos. Con objeto de preservar su margen de supervivencia, las personas limitadas en su posibilidad de escapar tuvieron que concebir una manera de resolver la nueva desfavorable ecuación de “luchar o huir”. Los seres humanos aprendieron rápidamente que la mera existencia de medidas protectoras era frecuentemente suficiente para descorazonar a los adversarios con

intenciones agresivas. Dolorosas experiencias enseñaron a los atacantes que buscaban penetrar las organizadas defensas que las pérdidas eran a menudo inaceptables y frecuentemente fueron disuadidos de nuevos ataques.

El próximo paso en la evolución de la Seguridad fue la emergencia de la especialización, primero por la división entre la seguridad interna y externa, y después entre la seguridad privada y pública. Con la aparición del estado y la confianza de su defensa a un organizado ejército, la responsabilidad de la seguridad interna se relevó gradualmente de la fuerza militar a la fuerza civil.

La seguridad pública estaba, basada en la seguridad interna. Ambas eran principalmente consideradas por los legisladores por el rol que podían jugar en la estabilidad de los gobiernos, en su propia seguridad. Una posible explicación es que la seguridad fue generalmente interpretada a través de los siglos más un bien privado que público.

La primera evidencia de una cultura y organización en seguridad madura aparece en el examen de los documentos y en la arqueología de la Roma imperial y republicana. Securitas Pública, en el sentido de “safety” o inmunidad del estado, adquirió una prominencia política y se plasmó en emblemas y monedas.

Agencias y cuerpos organizados, cuyas funciones eran similares a sus equivalentes modernos, garantizaban la seguridad pública. La protección de las costas y del tráfico naval contra la piratería fue asegurada por una potente flota, que precedió a la británica, que envolvía al Imperio. Sin embargo, ni incluso tal escudo gubernativo, sin precedentes en la antigüedad, pudo proveer a los ciudadanos de una completa seguridad. Pruebas pueden ser encontradas en Plauto, Cicerón, este último, aplaudía el asesinato cuando convenía a sus propios intereses. El uso de guardias de seguridad, guardaespaldas, perros de guardia, cajas fuertes, cerraduras y barrotes crearon las bases de la seguridad privada en la antigua Roma de forma notablemente similar a la de tiempos contemporáneos.

La seguridad pública se convirtió en una especie de asunto personal del jefe social, quien actuaba a la vez de legislador, juez, guardia y verdugo. Se confinó a

leyes rudimentarias y edictos, y principalmente confiada a vigilantes nocturnos, muros, puentes elevadizos y fosos de agua. Esencialmente a la habilidad de las personas de cuidarse a si mismas. En estas condiciones, la seguridad privada fue confiada a defensas físicas, a la habilidad de crear milicias privadas, a la fuerza de la familia y su habilidad de manejar armas.

Desde el siglo XVIII, los descubrimientos científicos y la extensión de conocimiento resultante de la invención de la imprenta han traído nuevas contribuciones a la cultura de seguridad. Laplace y sus principios de probabilidad, Bayes y su teorema de la predicción, las teorías de Gauss y Kolmogorov sobre la medición, han dado una base más científica tanto al concepto de reducción de pérdida como a la predicción de daños y fallos dentro de un sistema, incluyendo un sistema de seguridad.

Hoy, la seguridad, desde el punto de vista técnico, está en manos de la dirección de las organizaciones y, en última instancia, en cada uno de nosotros y en nuestro grado de concientización respecto a la importancia de la información y el conocimiento en este nuevo milenio.

1.2.1.2 DEFINICIÓN DE SEGURIDAD

Para la **[Real Academia Española, 2006],** la palabra Seguridad significa: “Que asegura algún buen funcionamiento, precaviendo que este falle, se frustre o se violente”.

Según **[Encarta, 2006]** el termino Seguridad significa. “(Del lat. securĭtas, -ātis). f. Cualidad de seguro. || 2. Certeza (‖ conocimiento seguro y claro de algo). || 3. Fianza u obligación de indemnidad a favor de alguien, regularmente en materia de intereses. || ~ jurídica. f. Cualidad del ordenamiento jurídico, que implica la certeza de sus normas y, consiguientemente, la previsibilidad de su aplicación. En España es un principio constitucional. || ~ social. f. Organización estatal que se ocupa de atender determinadas necesidades económicas y sanitarias de los ciudadanos. || de ~. loc. adj. Dicho de un ramo de la Administración Pública: Cuyo fin es el de

velar por la Seguridad de los ciudadanos. Agente de seguridad. || 2. Dicho de un mecanismo: Que asegura algún buen funcionamiento, precaviendo que este falle, se frustre o se violente. Muelle, cerradura de seguridad. □ V. beneficiario de la ~ social, cinturón de ~, guardia de ~, lámpara de ~, mecha de ~, medidas de ~, válvula de ~".

Para **[Diccionario Online, 2006**] La palabra Seguridad tiene varios significados:

- Certeza, certidumbre, fijeza [*], solidez, convicción, convencimiento, persuasión, evidencia, incertidumbre, inseguridad.

- Firmeza, estabilidad, confianza, fe [*]; desconfianza, inseguridad, irritabilidad ,

- Fianza, garantía, caución.

Atendiendo a estas definiciones, podemos decir que la Seguridad ha ido evolucionando en el transcurso del tiempo y se ha convertido en un término a tener en cuenta muy seriamente en el siglo XXI, ya que la confianza, firmeza, y garantía de mantenernos seguros va desde la seguridad de los ciudadanos como principio constitucional, hasta los más complejos mecanismos que aseguran un buen funcionamiento de todo un sistema.

1.2.1.3 CONCEPTO DE SEGURIDAD

De acuerdo a **[MORALES Silvia, 2006],** "la Seguridad debe ser interpretada como un estado subjetivo que nos permite percibir que nos desplazamos en un espacio exento de riesgos reales o potenciales".

De acuerdo a **[SANCHEZ, 2003],** "Seguridad es una necesidad básica de la persona y de los grupos humanos y al mismo tiempo un derecho inalienable del hombre y de las naciones. Seguridad proviene del latín SECURITAS, que a su vez se deriva del adjetivo SECURUS, sin cura, sin temor; implica las nociones de

garantía, protección, tranquilidad, confianza, prevención, previsión, preservación, defensa, control, paz y estabilidad de las personas y grupos sociales, frente a amenazas o presiones que atenten contra su existencia, su integridad, sus bienes, el respeto y ejercicio de sus derechos, etc.".

Según **[OLIVERA, 2006],** la seguridad es la interrelación dinámica (competencia) entre el agresor y el protector para obtener (o conservar) el valor tratado, enmarcada por la situación global". La seguridad trae consigo una ausencia de amenazas, situación que en el mundo contemporáneo es muy difícil de sostener, las sociedades actuales son crecientemente sociedades de riesgo. El componente riesgo es permanente y da carácter propio a los estados y sociedades nacionales, como tal la Seguridad no puede ser entendida como ausencia de amenazas".

[LARA, 2006] expresa que, "La Seguridad trae consigo una ausencia de amenazas, situación que en el mundo contemporáneo es muy difícil de sostener, las sociedades actuales son crecientemente sociedades de riesgo. El componente riesgo es permanente y da carácter propio a los estados y sociedades, como tal la Seguridad no puede ser entendida como ausencia de amenazas".

Analizando el criterio de varios autores, podemos concluir que la Seguridad es una necesidad indispensable de las personas, el estar seguro es muy difícil en los tiempos actuales, por eso conceptualmente no podemos analizar el término Seguridad como la ausencia total de amenaza, pero sí estar concientes de que los riesgos pueden minimizarse, esto equivaldría a más tranquilidad, confianza y control frente a las posibles amenazas.

1.2.2 SEGURIDAD INFORMÁTICA

En términos generales, la Seguridad puede entenderse como aquellas reglas técnicas y/o actividades destinadas a prevenir, proteger y resguardar lo que es considerado como susceptible de robo, pérdida o daño, esta abarca múltiples y muy diversas áreas relacionadas con los Sistemas de Información. Áreas que van desde la protección física del ordenador como componentes del hardware, de su

entorno, hasta la protección de la información que contiene o de las redes que lo comunican con el exterior.

1.2.2.1 DEFINICIÓN DE SEGURIDAD INFORMÁTICA

Sin embargo según plantea el **[Decreto-Ley No. 199]**, "Seguridad Informática es un conjunto de medidas administrativas, organizativas, físicas, técnicas, legales y educativas dirigidas a prevenir, detectar y responder a las acciones que puedan poner en riesgo la confidencialidad, integridad y disponibilidad de la información que se procesa, intercambia, reproduce o conserva por medio de las tecnologías de información".

En el artículo de **[Wikipedia, 2006]**, se formula que "la seguridad Informática, generalmente consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió".

Para **[Todos@cicese, 2002],** "Seguridad Informática es el conjunto de recursos (métodos, documentos, programas y dispositivos físicos) encaminados a lograr que los recursos de cómputo e información, disponibles en un ambiente dado, sean accedidos única y exclusivamente por quienes tienen la autorización para hacerlo".

[AUDITORIASISTEMAS, 2004], exponen "la Seguridad Informática es el conjunto de reglas, planes y acciones que permiten asegurar la información contenida en un sistema computacional."

En **[PC-News, 1996-2006],** se plantea a la Seguridad Informática como,"el conjunto de reglas, planes y acciones que permiten garantizar la prestación de servicios y asegurar la información contenida en un sistema computacional".
A partir de estas definiciones podemos decir que la Seguridad Informática es un conjunto de métodos y herramientas destinados a proteger la información y por

ende los sistemas informáticos ante cualquier amenaza, un proceso en el cual participan las demás personas.

1.2.2.2 CONCEPTOS DE SEGURIDAD INFORMÁTICA

Según manifiesta **[BRITIX, 2006]**, "Seguridad Informática son técnicas desarrolladas para proteger los equipos informáticos individuales y conectados en una red frente a daños accidentales o intencionados".

En el articulo de **[BLANCO, 2005]**, "La Seguridad Informática es un proceso complejo que conlleva tres aspectos: Gente, procesos y tecnología. Si estas variables no se evalúan y resuelven como partes de un todo, se obtiene como producto final un potencial o real desastre".

Como dijera [**PÉREZ**, **2006**], "La Seguridad de la Información sirve para abrir puertas, no para cerrarlas, evidentemente, la idea es abrir la puerta sólo a quién se le tiene que abrir".

Como expresara **[DÍAZ, 2004]**, en la conferencia titulada "La Seguridad Informática resulta imprescindible en esta 3ra. Revolución de la humanidad", "alcanzar el 100% de seguridad es imposible, pero los riesgos se pueden identificar, valorar, eliminar, minimizar, manejar y aceptar".

Cuando hablamos de "Seguridad", inmediatamente pensamos en puertas enrejadas, policías, alarmas, candados, etc. Todo parece llevarnos a asociar el concepto o la definición de "Seguridad" con el de "limitar", "restringir" o "prohibir". Evidentemente estos matices se encuentran implícitos, pero es necesario tener en cuenta también a la "Seguridad", y concretamente a la "Seguridad de la Información", no solo como un medio, sino como un fin, que nos permita establecer mecanismos de seguridad para mantener una imagen de los procesos dentro y hacia el exterior de nuestra institución, sin poner en peligro la información, ni los sistemas implicados, pero que nos permita conducir la

Seguridad como un medio para “habilitar” nuevas aplicaciones y extender todos los recursos de la información hacia entornos abiertos y disponibles. [**DÍAZ, 2006**]

Resumiendo lo expresado por **[BALUJA, 2000]**, la Seguridad Informática maneja tres conceptos básicos importantes para la seguridad de la información, en particular, en lo relativo a la seguridad en Internet, o en redes de datos. Estos son: confidencialidad, integridad y disponibilidad. Con respecto a los usuarios pudieran mencionarse otros como autenticación, autorización, contabilidad y no repudio.

La confidencialidad requiere que la información sea accesible únicamente por las entidades, sistemas o personas autorizadas. La confidencialidad de la información se aplica a todos los datos intercambiados por las entidades autorizadas o tal vez a sólo porciones o segmentos seleccionados de los datos, mediante cifrado. La confidencialidad de flujo de tráfico protege la identidad del origen y destino del mensaje.
La integridad requiere que la información solo pueda ser modificada por las entidades, sistemas, o personas autorizadas. La modificación incluye escritura, cambio, borrado, creación y reactuación de los mensajes transmitidos. La integridad de la información asegura que los datos recibidos no han sido modificados de ninguna manera.

La disponibilidad significa que la información no puede obtenerse por parte de aquellos que están autorizados y la necesitan. Para lograr que la información esté disponible para estos que tienen que confiar en ella se utilizan mecanismos de autenticación y autorización.

La autenticación se encarga de probar que cada usuario es quien dice ser. Este aspecto requiere una identificación correcta del origen del mensaje, asegurando que la entidad o usuario no sean falsos.

Los sistemas se hacen mucho más seguros si esa autenticación no puede ser refutada después o sea, si el usuario no puede esquivar ninguna responsabilidad en las acciones que desarrolló dentro de un sistema.

Esto se conoce como no repudio de la identidad. Este ofrece protección a un usuario frente a otro que niegue posteriormente que en realidad se realizó cierta comunicación. El no repudio de origen protege al receptor de que el emisor niegue haber enviado el mensaje, mientras que el no repudio de recepción protege al emisor de que el receptor niegue haber recibido el mensaje.

La contabilidad, se basa en el registro de todas las actividades que ocurren en el sistema. Cada proceso de autenticación y autorización son registrados con un nivel de información acorde a la configuración del sistema, mediante la contabilidad es posible saber cuál y cómo es el uso del sistema; puede conocerse qué preferencias tienen los usuarios y qué infracciones cometen.

Según **[BRADANOVIC Tomás, 2006]**, estos conceptos son analizados como principios elementales:

Confidencialidad

La confidencialidad o privacidad es el más obvio de los aspectos y se refiere a que la información solo puede ser conocida por individuos autorizados. Existen infinidad de posibles ataques contra la privacidad, especialmente en la comunicación de los datos. La transmisión a través de un medio presenta múltiples oportunidades para ser interceptada y copiada: las líneas "pinchadas", la intercepción o recepción electromagnética no autorizada, o la simple intrusión directa en los equipos donde la información está físicamente almacenada.

Integridad

La integridad se refiere a la Seguridad de que una información no ha sido alterada, borrada, reordenada, copiada, etc., ó bien durante el proceso de transmisión o en su propio equipo de origen. Es un riesgo común que el atacante al no poder descifrar un paquete de información y, sabiendo que es importante, simplemente lo intercepte y lo borre.

Disponibilidad

La disponibilidad de la información se refiere a la seguridad de que la información pueda ser recuperada en el momento que se necesite, esto es evitar su pérdida o bloqueo, bien sea por ataque doloso, mala operación accidental o situaciones fortuitas o de fuerza mayor.

Como expresa **[VELÁZQUEZ, 2006]**, "Existen tres principios claves en esta materia que se consideran importantes: confidencialidad, integridad y disponibilidad:

La confidencialidad, previene la divulgación ya sea intencional o por negligencia, del contenido de un mensaje, archivo, correo, etcétera.

La integridad, por otro lado, asegura que nadie pueda modificar datos confidenciales, específicamente por personas no autorizadas. También evita a quienes tienen privilegios de realizar las modificaciones, o lo hagan sin autorización; finalmente lo más importante es que los datos sean consistentes es decir, que la información refleje la verdad.

La disponibilidad asegura que la información esté a la mano cuando sea necesario en tiempo y espacio, para las personas que la requieren. En otras palabras, la disponibilidad garantiza que los sistemas funcionen cuando se necesitan".

Con respecto a estos conceptos, la seguridad Informática pretende identificar los riesgos de la información y constatar los problemas que son de vital importancia para dar a conocer a las personas que en la actualidad se viene trabajando en normalizar los aspectos más importantes para garantizar la disponibilidad, la integridad y confiabilidad de los sistemas de información.

Con los principios analizados anteriormente y para tener una idea mas clara, señalaremos algunas definiciones:

Autenticación:

- Procedimiento de comprobación de la identidad de un usuario. **[DECRETO-LEY No. 199]**
- Característica de dar y reconocer la autenticidad de los activos del dominio (de tipo información) y/o la identidad de los actores y/o la autorización por parte de los autorizadores, así como la verificación de dichas tres cuestiones. **[MAGERIT. Versión 1.0]**
- Servicio de seguridad que se puede referir al origen de los datos o a una entidad homóloga. Garantiza que el origen de datos, o entidad homóloga, son quienes afirman ser. **[ISO 7498-2]**

Confidencialidad:

- Condición que asegura que la información no puede estar disponible o ser descubierta por o para personas, entidades o procesos. La confidencialidad a menudo se relaciona con la intimidad cuando se refiere a personas físicas. **[MAGERIT. Versión 1.0]**
- Propiedad de la información que impide que esta esté disponible o sea revelada a individuos, entidades o procesos no autorizados. **[ISO 7498-2]**
- Prevención de la revelación no autorizada de información. **[ISO/IEC TR 13335]**

Integridad:

- Condición de seguridad que garantiza que la información es modificada, incluyendo su creación y borrado, sólo por el personal autorizado. La integridad está ligada a la fiabilidad funcional del sistema de información, a su eficacia para cumplir las funciones del sistema. **[MAGERIT, Versión 1.0]**
- Propiedad de los datos que garantiza que éstos no han sido alterados o destruidos de modo no autorizado. **[ISO 7498-2]**.

- Seguridad de que la información o los datos, están protegidos contra modificación o destrucción no autorizada y certidumbre de que los datos no han cambiado de la creación a la recepción. Prevención de la modificación no autorizada de información. **[ISO/IEC TR 13335]**

1.3 ¿POR QUÉ ES IMPORTANTE LA SEGURIDAD INFORMÁTICA?

Las personas ajenas a la información, también conocidas como piratas informáticos, buscan tener acceso a la red para modificar, sustraer o borrar datos, así como también estos pueden ser parte del personal administrativo o de sistemas, de cualquier organización. De acuerdo a estudios realizados la mayor parte de las violaciones e intrusiones a los recursos informáticos se realiza por el personal interno, debido a que éste conoce los procesos, metodologías y tiene acceso a la información sensible es decir, a todos aquellos datos cuya pérdida puede afectar el buen funcionamiento de la organización.

Las causas fundamentales que llevan a este problema es la ineficiencia de la seguridad que está presente en la mayoría de las compañías y organizaciones a nivel mundial, y que no existe conocimiento relacionado con la planeación de un diseño de Seguridad eficiente que proteja los recursos informáticos de las actuales amenazas combinadas.

El resultado de todo esto es la violación realizada a los sistemas, provocando la pérdida o modificación de los datos o informaciones sensibles de cualquier organización, lo que puede representar un daño económico de gran magnitud.

Por tal razón, la información, como los sistemas informáticos deben estar protegidos ante cualquier ataque externo o interno que pretenda robar, alterar o destruir la información, o inutilizar temporalmente los equipos informáticos.

En base a lo anterior, afirmamos que no se puede dogmatizar que la seguridad perfecta existe, lo afirme quien lo afirme. Pero, al menos, sí se pueden adoptar medidas preventivas a cada una de sus actividades.

1.3.1 ¿QUÉ DEBEMOS PROTEGER?

En cualquier sistema informático existen tres elementos básicos a proteger: el hardware, el software y los datos.

Por hardware entendemos el conjunto de todos los sistemas físicos del sistema informático: CPU, cableado, impresoras, CD-ROM, cintas, componentes de comunicación, etc.

El software son todos los elementos lógicos que hacen funcionar al hardware: sistema operativo, aplicaciones, utilidades, etc.

Entendemos por datos al conjunto de información lógica que maneja el software y el hardware: bases de datos, documentos, archivos, etc.

Generalmente se habla de un cuarto elemento llamado fungible; aquellos que se gastan o desgastan con el uso continuo: papel, tonner, tinta, cintas magnéticas, disquetes, etc.

De los cuatro, los datos que maneja el sistema serán los más importantes ya que son el resultado del trabajo realizado. Si existiera daño del hardware, software o de los elementos fungibles, estos pueden adquirirse nuevamente desde su medio original; pero los datos obtenidos en el transcurso del tiempo por el sistema son imposibles de recuperar.

1.3.2 ¿DE QUIÉN PROTEGERSE?

Para orientar la perspectiva de quien protegerse, inicialmente debe existir un conocimiento claro y preciso de lo que significa un ataque.
Según **[Encarta, 2006],** "ataque. m. Acción de atacar, acometer o emprender una ofensiva. || 2. Acción de atacar, perjudicar o destruir. || 3. En algunos deportes, iniciativa que toma un jugador o un equipo para vencer al adversario. || 4. Acceso repentino ocasionado por un trastorno o una enfermedad, o bien por un sentimiento extremo. Ataque de nervios, de ira. Ataque al corazón. || 5.

Impugnación, crítica, palabra o acción ofensiva. || 6. Desus. Conjunto de trabajos de trinchera para tomar o expugnar una plaza. □ V. paso de ~.".

Por consiguiente, la seguridad de los sistemas de información está amenazada por un creciente número de ataques, es decir, cualquier acción podría dar lugar a que se produjese una violación de la seguridad de la información (confidencialidad, integridad, disponibilidad o uso legítimo).

Como señala **[MURILLO, 2005],** las cuatro categorías generales de amenazas o ataques son las siguientes:

Interrupción: Un recurso del sistema es destruido o se vuelve no disponible. Este es un ataque contra la disponibilidad. Ejemplos de este ataque son la destrucción de un elemento hardware, como un disco duro, cortar una línea de comunicación o deshabilitar el sistema de gestión de archivos.

Modificación: Una entidad no autorizada no solo consigue acceder a un recurso, sino que es capaz de manipularlo. Este es un ataque contra la integridad. Ejemplos de este ataque es el cambio de valores en un archivo de datos, alterar un programa para que funcione de forma diferente o modificar el contenido de mensajes que están siendo transferidos por la red.

Fabricación: Una entidad no autorizada inserta objetos falsificados en el sistema. Este es un ataque contra la autenticidad. Ejemplos de este ataque son la inserción de mensajes esporádicos en una red o añadir registros a un archivo.

Estos ataques se pueden clasificar de la misma forma útil en términos de ataques pasivos y activos.

Ataques pasivos

En los ataques pasivos el atacante no altera la comunicación, sino que únicamente la escucha o monitorea, para obtener información que está siendo transmitida. Sus objetivos son la intercepción de datos y el análisis de tráfico, una

técnica más sutil para obtener información de la comunicación, que puede consistir en:

- Obtención del origen y destinatario de la comunicación, leyendo las cabeceras de los paquetes monitoreados.
- Control del volumen de tráfico intercambiado entre las entidades monitoreadas, obteniendo así información acerca de actividad o inactividad inusuales.
- Control de las horas habituales de intercambio de datos entre las entidades de la comunicación, para extraer información acerca de los períodos de actividad.

Estos ataques son muy difíciles de detectar, ya que no provocan ninguna alteración de los datos.

Ataques activos

Estos ataques implican algún tipo de modificación del flujo de datos transmitido o la creación de un falso flujo de datos, pudiendo subdividirse en cuatro categorías:

- **Suplantación de identidad:** el intruso se hace pasar por una entidad diferente. Normalmente incluye alguna de las otras formas de ataque activo. Por ejemplo, secuencias de autenticación pueden ser capturadas y repetidas, permitiendo a una entidad no autorizada acceder a una serie de recursos privilegiados reemplazando a la entidad que posee esos privilegios, como al robar la contraseña de acceso a una cuenta

- **Reactuación:** uno o varios mensajes legítimos son capturados y repetidos para producir un efecto no deseado, como por ejemplo ingresar dinero repetidas veces en una cuenta dada.

- **Modificación de mensajes:** una porción del mensaje legítimo es alterada, o los mensajes son retardados o reordenados, para producir un efecto no

autorizado. Por ejemplo, el mensaje "Ingresa un millón de pesos en la cuenta A" podría ser modificado para decir "Ingresa un millón de pesos en la cuenta B".

- **Degradación fraudulenta del servicio:** impide o inhibe el uso normal o la gestión de recursos informáticos y de comunicaciones. Por ejemplo, el intruso podría suprimir todos los mensajes dirigidos a una determinada entidad o se podría interrumpir el servicio de una red inundándola con mensajes esporádicos. Entre estos ataques se encuentran los de denegación de servicio, consistentes en paralizar temporalmente el servicio de un servidor de correo, Web, FTP, etc.

De lo que expresa el artículo de **[TRUKULO, 2003]**, podemos resumir que existen muchas razones por lo que las personas pueden motivarse para realizar los ataques, a partir de ello se habla de dos tipos diferentes, que están condicionados por las acciones realizadas después de la intrusión, denominado "ataque hacker": este se realiza saltando las barreras de seguridad, borrando las huellas y saliendo sin hacer daño a la empresa o al usuario al que pertenece el equipo asaltado. En este tipo de ataque, el agresor esta motivado por aprender sobre seguridad informática: quizás quiera saber
como está montada la red a la que esta accediendo, etc., pero sin la intención de causar daño, por eso sólo modificará lo necesario para no ser encontrado.

El otro tipo de ataque es el llamado "ataque cracker": un ataque con motivos económicos, (robar dinero, conseguir información, etc.), por venganza o simplemente por afán de destruir.

Los dos atacantes pueden tener los mismos conocimientos pero mientras el primero los usa como es debido el segundo los usa para hacer daño.

Hay demasiados ejemplos de ataques como para nombrarlos o explicarlos, por tal motivo nos limitamos a explicar los más comunes y generales:

dDOS : Denegación de servicio. Este ataque es uno de los más usados por los crackers, no tienen mérito alguno y lo que se consigue normalmente es hacer caer a la máquina contra la que se realiza.

Sniffing : El arte del sniffing es muy usado por los hackers. Consiste en filtrar todos los paquetes que pasan por una red abriendo cada uno de ellos para mirar el interior, en busca de contraseñas o información útil.

Troyano: Consiste en un programa que simula ejecutar una función mientras que realmente ejecuta otra (por eso es llamado Caballo de Troya). Normalmente la tarea secundaria del troyano consiste en dar un control e inmovilizar el ordenador víctima, etc. Este es un ataque muy expandido pero no tendría que causar demasiados destrozos, ya que un equipo mínimamente protegido puede repeler estos ataques.

Xploits: Estos son programas que se aprovechan de algún tipo de vulnerabilidad en el sistema donde se usan y mayoritariamente sirven para ganar privilegios en el equipo.

Fuerza bruta: Aunque estos términos pueden generalizar mucho, aquí se resaltan, el uso de programas que mandan contraseñas con nombres de usuarios consecutivamente hasta conseguir acceso a una máquina.

1.3.3 CLASIFICACIÓN DE LOS INTRUSOS DE ACUERDO AL NIVEL DE CONOCIMIENTO

Desde hace algunos años, con el vertiginoso avance de las comunicaciones y el trascendental uso del Internet, se han originado múltiples actos ilícitos, o los comúnmente denominados “ataques informáticos”, que con intención o sin ella, se han convertido en violaciones a los sistemas informáticos, causando perjuicios a sus recursos y en la mayoría de los casos produciendo pérdidas económicas a las empresas u organizaciones que han sido víctimas de estas agresiones. Por ello, para hablar de “intrusos” realizaremos la siguiente propuesta con un enfoque

determinado al nivel del conocimiento informático que cada uno de estos posee, tomando como referencia los siguientes puntos de vista.

Nivel básico:

En este contexto caracterizaremos a los usuarios que poseen un conocimiento limitado, con respecto a determinadas debilidades de los sistemas y el uso de herramientas informáticas, pero que de alguna forma logran tener acceso fácil a determinada información de manera ilícita, estos casos pueden acontecer cuando las personas acceden y navegan por las páginas del Internet y tienden a realizar pruebas de programas informáticos de los cuales no tiene pleno conocimiento acerca de los daños que pueden causar. Dentro de este conjunto podemos valorar un porcentaje aceptable de intrusión, con un 70% debido al total desconocimiento de lo que realizan.

Nivel medio:

En este grupo examinaremos los delitos de arduo descubrimiento, donde los intrusos ya desarrollan programas de intrusión para ser ejecutados , conocen como detectar el sistema operativo que está usando la víctima, testean y bucean en las vulnerabilidades del mismo, ingresan en varios casos sin respetar las restricciones de usuarios u contraseñas, pero sus objetivos no están al 100% establecidos, motivo por el cual sus ataques pueden decaer en el intento, ya que no gozan de un amplio conocimiento, con este análisis podemos apreciar que un 25% de ataques son producidos por aquellas personas que trabajan internamente en organizaciones y existe una cooperación entre empleados y terceros, los cuales conocen la configuración interna de sus plataformas o su funcionamiento básico y se encuentran interesadas en romper las barreras de seguridad.

Nivel avanzado:

Comprende todas aquellas personas con conductas dirigidas en algunos casos a causar daños, en el hardware o en el software de un sistema, pero ya en una

forma especializada, mediante estudios realizados se evalúa que los métodos utilizados para causar destrozos en los sistemas informáticos son de variada índole en cada una de sus categorías y han ido evolucionando hacia técnicas cada vez más sofisticadas y de difícil detección.

Hoy en día, el llamado “phishing” constituye unos de los ataques con mayor índice en el mundo entero por los intrusos informáticos, esta forma de ataque llega en mensajes de correo electrónico y se difunde por la red; los atacantes deben tener un pleno conocimiento para realizar esta actividad.

Por ello, según un análisis personal podemos comentar que hasta la actualidad existe una cifra que sobrepasa los 100.000 intrusos especializados que plenamente dominan el tema ,de los cuales según nuestro criterio solo un 0,02 son profesionales, constituyendo un 2% que se guían directamente a su objetivo como un trabajo de lucro netamente económico, el otro subgrupo lo constituiremos con un 0,03 equivalente a un 3%, estos son intrusos que con ayuda de sus conocimientos informáticos consiguen acceder a distintos servidores u ordenadores ya sea de los bancos o de organismos públicos o privados, exploran la información que no les pertenece, roban software caro en varios casos o realizan transacciones de una cuenta bancaria a otra, todo esto con el afán de sondear información secreta o romper la seguridad que estos poseen y en casos especiales pueden generar un impacto a largo plazo, estos intrusos lo realizan en varios casos por satisfacción personal ya que para ellos no existe límite en la palabra “Seguridad”. Estos dos grupos integran un total del 5% de usuarios que poseen un dominio pleno de la materia.

En el siguiente gráfico se puede observar los tipos de Intrusos, definidos desde el nivel del conocimiento informático.

CLASIFICACIÓN DE LOS INTRUSOS DE ACUERDO AL NIVEL DE CONOCIMIENTO

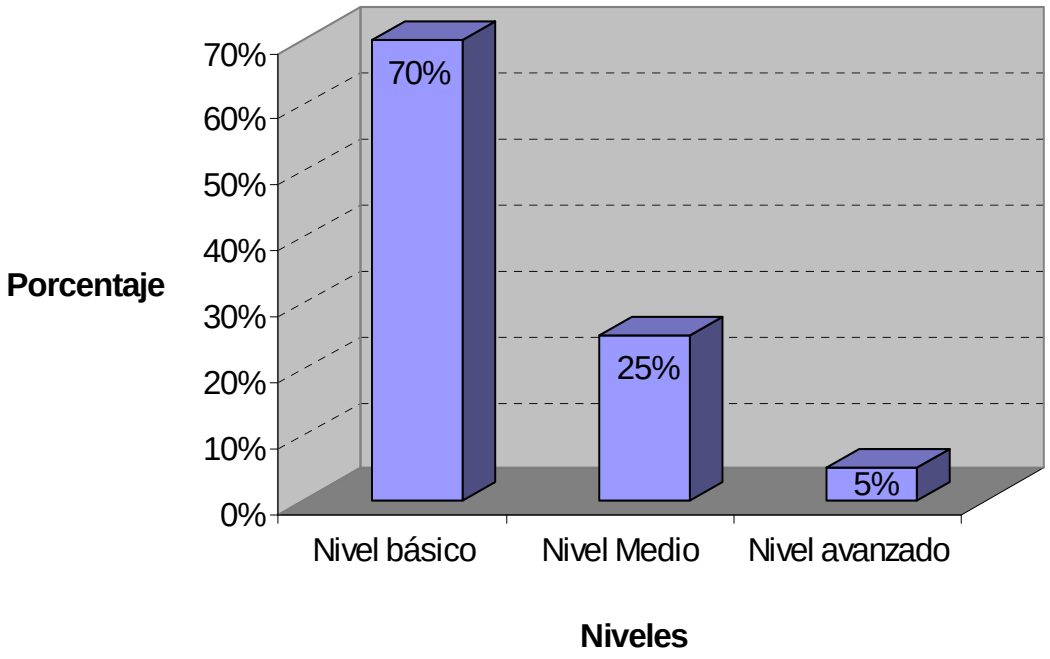

FIG I. 1.3.3 Clasificación de Intrusos

1.4 MÉTODOS DE SEGURIDAD

Como señala **[BADOPI, 2003]**, para tener una buena seguridad ante los ataques tenemos que tener en cuenta tres factores principales: la prevención, la recuperación y la detección.

Prevención

La prevención se encarga de preparar el equipo para recibir los ataques, mantener una buena política de seguridad y poder reaccionar al momento, para así evitar el ataque. Con la prevención podemos encontrar los firewalls, IDS, etc, que son lo que nos ayuda a evitar el ataque. Dentro de prevención podemos encontrar también todo lo que se refiere a hacer unas buenas copias de

seguridad, mantener diferentes equipos encargándose de la seguridad a la vez, etc.

Detección

La detección se encarga de detectar los ataques en el momento que se están realizando, y así poder contrarrestarlos debidamente. Un ejemplo de detección seria un IDS bien configurado, que sepa al momento lo que está ocurriendo y nos avise debidamente.

Recuperación

Esta es la parte más crítica, cuando no se ha logrado evitar el ataque, y consiste en recuperar todo el equipo como lo teníamos en un inicio borrando el ataque para poder continuar normalmente.

1.5 MECANISMOS DE DEFENSA

[GONZÁLEZ, 2004], explica “que no existe un único mecanismo capaz de proveer todos los servicios anteriormente citados”, pero los más importantes son los siguientes:

Encripción

La criptografía es el arte de escribir en secreto, de transformar un texto simple a un párrafo ilegible con lo que se asegura que solo la persona que tenga la llave para leer el mensaje lo hará. Es aún la herramienta más poderosa para proporcionar seguridad computacional, al hacer que un texto sea ininteligible para el observador externo se logra que se nulifique el valor de una intercepción de los mensajes y la posibilidad de que estos sean modificados o fabricados.

Controles de Software

Los programas deben de ser lo suficientemente seguros para excluir los ataques desde afuera. También deben de ser diseñados y mantenidos para que uno pueda tener confianza en la seguridad de los programas. Los controles de software pueden incluir lo siguiente:

- Controles internos de programa
- Controles al sistema operativo
- Controles de desarrollo

Controles de Hardware

Han sido ya diseñados numerosos dispositivos que asisten en la seguridad computacional, estos van desde implementaciones de encripción en el hardware o en smartcards para asegurar el acceso limitado, protección al robo, hasta dispositivos que verifican las identidades de los usuarios.

Autenticación e identificación.

Este mecanismo hace posible identificar entidades del sistema de una forma única, y posteriormente, una vez identificadas, autenticarlas (comprobar que la entidad es quién dice ser).

Políticas

Son los controles que a través de la administración y entrenamiento inmediato pueden prevenir distintas amenazas que pueden presentarse en los sistemas o recursos de información.

Firma digital

Este mecanismo implica el cifrado, por medio de la clave secreta del emisor, de una cadena comprimida de datos que se va a transferir. La firma digital se envía

junto con los datos ordinarios. Este mensaje se procesa en el receptor, para verificar su integridad. Juega un papel esencial en el servicio de no repudio.

Esteganografia

Esta técnica consiste precisamente en ocultar un texto o cualquier otra información, dentro de un archivo de gráfico o de audio, asegurado con una clave de acceso solo conocida por la persona que cree dicho archivo, quien también será el encargado de hacerla saber a quien tenga que descubrir el contenido de dicha foto o audio, sin la cual sería casi imposible de obtener.

Tráfico de relleno

Consiste en enviar tráfico espurio junto con los datos válidos para que el atacante no sepa si se está enviando información, ni qué cantidad de datos útiles se está transmitiendo.

Control de encaminamiento

Permite enviar determinada información por determinadas zonas consideradas clasificadas. Asimismo posibilita solicitar otras rutas en caso que se detecten persistentes violaciones de integridad en una ruta determinada.

Unicidad

Consiste en añadir a los datos un número de secuencia, la fecha y hora, un número aleatorio, o alguna combinación de los anteriores, que se incluyen en la firma digital o integridad de datos. De esta forma se evitan amenazas como la reactuación de mensajes.