8

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE CONTADURIA Y ADMINISTRACION

"ANALISIS DE RIESGOS EN CENTROS DE COMPUTO"
(TAXONOMIA PROPUESTA DE ATAQUES A COMPUTADORAS Y A REDES DE COMPUTADORAS)

TESIS PROFESIONAL

QUE PARA OBTENER EL TITULO DE

LICENCIADO EN INFORMATICA

PRESENTA:

VICTOR LOPEZ GUERRERO

DIRECTOR DE TESIS:
DR. RICARDO RIVERA SOLER

2495

MEXICO, D. F. **200**

Agradecimientos.

A la profesora Teresa García

Por enseñarme a leer y a escribir, y con ello mostrarme la mitad del mundo.

"La seguridad somos todos"
Lic. Rosario Robles
Jefa de Gobierno del D.F.
(1998-2000)

INDICE

CONTENIDO.

III. Marco conceptual

IV. Marco metodológico

V. Marco instrumental.

VI. Conclusiones.

VII. Glosario y abreviaturas.

INTRODUCCIÓN.

En la empresa actual el valor más importante radica en la información. Han pasado ya los tiempos en que los elementos productivos eran la base efectiva del negocio y hoy, más importante que las máquinas es la información que permite saber qué, cómo y cuándo hacer algo. Desde el momento en que las empresas destinan importantes sumas de dinero a cuidar su seguridad, resulta evidente que por algo lo harán. Y ese algo es que muchas empresas han sufrido el daño que causa una no disponibilidad de la información.

El principal problema que plantea esta cuestión es que las personas están de acuerdo en que la falta de control sobre la información es un riesgo latente, pero muchas de ellas ven difícil la materialización del mismo en un momento dado. Que en un determinado momento no se den las circunstancias propicias para temer un intento de acceso a nuestra información interna no significa que éste no vaya a producirse, ello independientemente de que el número de posibles amenazas es, generalmente, desconocido por nosotros mismos.

Las medidas de seguridad para computadoras y redes de computadoras pueden ser tan sencillas o tan complejas como se desee o se pueda permitir. Todas las personas que laboran en un centro de cómputo podrían tomar medidas básicas para crear contraseñas seguras, no dejar impresos con claves en cualquier lado y podrían mantener el hardware seguro y contar con datos delicados cifrados.

Es evidente que alguien podría estar interesado en la información que se genera en la empresa. Como ejemplos se encontraría la competencia, un trabajador resentido, un periodista ávido de escándalos, un grupo de investigación, un miembro de nuestro propio equipo de trabajo, etc., todos, podrían estar interesados en determinada información, sea para fines lícitos o ilícitos.

Son tantos y tan variados esquemas de inseguridad que podrían afectar a la información que su utiliza en una computadora o en una red de computadoras que varios autores han tratado de clasificar a los ataques y a las vulnerabilidades computacionales de distintas maneras y van desde cuadros empíricos hasta clasificaciones detalladas basadas en determinado criterio.

Actualmente la tecnología permite llevar a cabo sistemas de espionaje con un ámbito extraordinario, de forma imperceptible. Baste como ejemplo señalar que, hoy en día, por unos cuantos pesos se puede adquirir en el mercado un equipo capaz de monitorear todas las conversaciones mantenidas a través de un teléfono, independientemente del lugar donde esté el usuario. Si comparamos estas cifras con el presupuesto invertido por las modernas compañías en estudios de mercado veremos lo irrisorio de su importe.

Pero, además, el riesgo no está, ni exclusiva ni principalmente, en el acceso de compañías competidoras a la información interna de ellas. Incluso en el seno de la propia empresa, un acceso incontrolado a la información es fuente de conflictos imprevisibles y, en la mayoría de los casos, de sospechas mutuas que enturbian el clima de trabajo.

Nadie puede valorar el efecto que producirá en un tercero una determinada información. Por ello, toda la información debe ser objeto de protección frente a fugas incontroladas. Incluso la que podría considerarse como inútil.

El presente estudio no es un plan de seguridad corporativa, sino simplemente tratará de convertirse en un documento de referencia que, a través de sus páginas llame la atención sobre las distintas etapas de manifestación del riesgo y ofrecer una serie de pautas basadas en una taxonomía inteligente para que usted lector pueda planear una estrategia de mitigación o prevención de riesgos.

En este trabajo se describen, clasifican y analizan todos los incidentes de seguridad computacional, localizados en su mayor parte en ambientes de red y que son aplicados a casi todo centro de cómputo de hoy en día.

La clave de la seguridad en materia de cómputo es la organización y vigilancia. Conforme el desarrollo de software y hardware lucha por construir trampas para ratones grandes, los ratones se vuelven cada vez más mas inteligentes y encuentran cada vez más nuevas y mejores medidas para evitar las trampas.

Este trabajo esta dividido en varias secciones, la parte I "Marco problemático" aborda los problemas de la seguridad en un centro de cómputo. Como se podría imaginar, una persona con malas intenciones se podría encontrar ante una fuga de datos y obtener aquellos que le pudieran servir o quizá a alguien más. Con ello se crea una hipótesis propuesta de trabajo y se indica además el interés detectado hasta el momento por las autoridades en nuestro país.

El capítulo II "Marco teórico" se bosqueja por tipos de referencias documentadas todo el conocimiento con respecto al tema de seguridad, riesgos, vulnerabilidades y ataques a la información. Se hace una descripción de lecturas tan representativas como el "orange book" y otros más.

El capítulo III "Marco conceptual" a través de un análisis profundo especifica una taxonomía de ataques a computadoras y a redes de computadoras. Muestra todos aquellos esfuerzos llevados a cabo por otros autores y se realizan algunas notas comparativas y notaciones al respecto.

En el capítulo IV "Marco metodológico" se llevan a cabo todos los pasos para desarrollar la hipótesis de trabajo. Se realiza la presentación del problema en sus causas y en sus efectos.

En el capítulo V "Marco instrumental" presenta algunas actividades que el autor propone para dar difusión a este tipo de problemáticas detectadas y algunas medidas de prevención.

En el capítulo VI "Conclusiones" presenta la conclusión general derivada de este trabajo.

En el capítulo VII se proporciona un glosario y una referencia de abreviaturas que fueron utilizados a lo largo de este trabajo.

Este trabajo pretende llegar a un amplio número de lectores, aquellos que se encuentran estudiando informática y a todos aquellos interesados en los tópicos de seguridad informática.

A lo largo de este trabajo se han colocado palabras que aparecen formateadas con letras *itálicos*. Tales palabras y/o abreviaturas se podrán encontrar en el glosario de términos o bien en el índice de abreviaturas y acrónimos al final de este trabajo.

Este trabajo no pretende ser un categorizador de riesgos en centros de computo, simplemente trata de establecer una clasificación de estudio para los mismos y con ello intentar establecer el primer cimiento para una clasificación inteligente de todos aquellos factores reales y potenciales que podrán afectar a nuestros equipos de cómputo.

I. MARCO PROBLEMÁTICO.

1.1. Antecedentes.

Hasta finales del siglo XVII las diferencias de país a país en cuanto a los recursos materiales de que disponían para vivir las mayorías, eran casi imperceptibles, su nivel de vida era apenas superior al de la mínima subsistencia en todas las sociedades. Con la primer revolución industrial esto cambio radicalmente, surgieron las disparidades cada vez más notorias entre los países pobres y los países ricos. Esto se debió en gran parte a los avances científicos y a la capacidad de cada sociedad para aprovecharlos, es decir a su desarrollo tecnológico.

Actualmente se puede leer mucho sobre la importancia de la informática para el desarrollo tecnológico de las sociedades modernas, de la revolución de la inteligencia. Comenzando el año 2000 surgen conceptos como: "knowledge management[1]" e "ingeniería del conocimiento[2]". Tanto se advierte de transformaciones radicales que ello puede fácilmente afectar la voluntad de la sociedad para enfrentar adecuadamente un reto que podría determinar el papel de la sociedad mexicana a partir de este momento.

Haciendo rápidamente una semblanza histórica se observaría que el cómputo ha cambiado dramáticamente en las últimas tres décadas y los cambios acontecen cada vez más rápido; como lo ha indicado ya el Dr. Alejandro Pisanty[3] en el evento para celebrar los 40 años de cómputo en México: "....incluso en un mismo año se puede pasar de la invención a la probabilidad de obsolescencia pasando por la innovación"[4].

En las últimas tres décadas del cómputo en México se pasó de unas cuantas computadoras a miles de ellas, de unos cuantos "genios" que sabían utilizar éstas máquinas de cálculo hasta el día de hoy en el que un niño de primaria puede encender, iniciar, y ejecutar un programa de computadora ya sea para construir pueblos como sucede en "Age of Empires", matar decenas de personas como en "Resident Evil" o simplemente utilizar un procesador de palabras para realizar su tarea.

La disposición física y lógica de las computadoras en los centros de cómputo también han sufrido demasiados cambios. En los años 70's muchas computadoras para realizar su procesamiento estaban basabas en una arquitectura centralizada y eran administradas por los centros de procesamiento de datos.

Las computadoras eran mantenidas en cuartos cerrados y grupos de personas tenían la responsabilidad de asegurarse que las computadoras estuvieran cuidadosamente administradas y físicamente seguras. Los enlaces a otros destinos fuera de los centros de cómputo eran poco usuales.

---

[1] http://www.km.org enlace visitado el día 17 de enero del 2000 y http://www.ckm.ucsf.edu/ visitado el día 2 de febrero del 2000.

[2] Nuevo concepto en ingeniería del software.

[3] Director de la *D.G.S.C.A.* hasta marzo del 2000.

[4] Número especial de la revista RV Celebración de los 40 años de cómputo en México.

Las amenazas hacia el equipo de cómputo en los centros de cómputo en ese esquema básicamente ocurrían por personas que laboraban dentro de este; personas que hacían un mal uso de sus cuentas de acceso o del equipo en general, ocurrencias de robo y vandalismo, etc. Estas amenazas eran bien conocidas y se reducían utilizando algunas técnicas sencillas de instrumentar: puertas que bloqueaban los accesos, registros de existencias de recursos de todo tipo, instalación de cámaras de vídeo dentro del centro de cómputo, etc.

El cómputo en los años 90's es radicalmente diferente. Muchos sistemas se encuentran en oficinas privadas y laboratorios, son administrados por individuos que pueden hacerlo interna o externamente al centro de cómputo. Muchos sistemas se encuentran conectados a internet y por lo tanto, con posibilidad de estar conectados simultáneamente con todo el mundo: Australia, Europa, Asia, África y el resto de América.

Esta capacidad de interconexión entre los distintos equipos de cómputo se conoce actualmente como "sistemas abiertos" [5]. Como tales, los sistemas abiertos están cimentados en una filosofía muy interesante: la compartición de recursos y servicios de manera local o remota, transparente y en cualquier momento.

Es precisamente ésta capacidad la que se vuelve bondad en un extremo pero inseguridad por el otro ya que se invita a quien necesite un servicio que se traslade hasta donde se encuentra el proceso servidor, demande un servicio, lo obtenga y se retire para que otros demandantes obtengan servicios similares. Existen además personas que intentan entrometerse a los sistemas computacionales para obtener algún satisfactor. En la era de los sistemas abiertos esas personas pueden encontrarse tan solo a un metro de distancia de la máquina objetivo o bien pueden encontrarse a varios cientos de kilómetros en la parte posterior del planeta.

Como se puede percibir, también los riesgos evolucionan, forman parte de la actualización tecnológica del cómputo. Siempre que hay un adelanto en el campo de la informática surge también una amenaza, siempre existirán personas que deseen obtener algún beneficio, surge en ese momento un riesgo en el centro de cómputo.

En este trabajo se define al riesgo como la posibilidad de que ocurra algún evento difícil de prever ocasionando un escenario que atente contra la operabilidad correcta de las empresas o de los actos de las propias personas. Prácticamente toda actividad conlleva de manera implícita una probabilidad de riesgo, manejar un automóvil, utilizar un cajero automático, confiar un equipo de cómputo a una persona, contar con instalaciones laborales en un país volcánico, etc. todo implica un cierto grado de riesgo.

[5] Sistema abierto.- En comunicaciones, una red de computadoras diseñada para incorporar todos los dispositivos, sin importar su fabricante o modelo, que pueden utilizar las mismas facilidades y los mismos protocolos. Definición del Computer Dictionary Microsoft 1997.

A últimas fechas se ha difundido demasiado la alerta y la necesidad de crear conciencia de las consecuencias derivadas por parte de las organizaciones de no dar la importancia suficiente a los riesgos en materia de cómputo, tal es así que se refleja el tema de seguridad en los eventos serios de cómputo y con cada vez más frecuencia en internet. La UNAM cuenta con uno de los equipos de trabajo más importantes en materia de seguridad en cómputo en México, el ASC (Área de Seguridad en Cómputo) quien además se encarga de dar difusión a la cultura de seguridad informática.

Existe una ampliación al modelo de referencia conocido como "*modelo OSI*" hecha por el *JTC1* de *ISO/IEC* quienes añadieron en 1989 una arquitectura de seguridad (*ISO/IEC*, 1989), e *ITU-T* adoptó dicha arquitectura en su recomendación X.800 (ITU, 1991). De echo, *ISO* 7498-2 e *ITU-T* X.800 describen la misma arquitectura de seguridad. En dicha recomendación se plantea la idea de contar con diversos *servicios de seguridad* para las aplicaciones informáticas.

Un *servicio de seguridad* es una funcionalidad abstracta que forma parte de la seguridad de un sistema. Tal servicio contrarresta *ataques* a la seguridad y utiliza una o más acciones de detección, prevención o recobro ante acciones que comprometen la seguridad de la información.

La arquitectura de seguridad *OSI* (estándares *ISO* 7498-2 e *ITU-T* X.800) distingue cinco clases de *servicios de seguridad*:

1. *Autenticación.*
   - *Autenticación* de entidad pareja.
   - *Autenticación* del origen de los datos.
2. *Control de acceso.*
3. *Confidencialidad* de los datos.
   - Orientado a conexión.
   - No orientado a conexión.
   - De flujo de datos.
4. *Integridad* de los datos.
   - Orientada a conexión con recuperación.
   - Orientado a conexión sin recuperación.
   - De campo seleccionado orientado a conexión.
   - No orientado a conexión.
   - De *integridad* de campo seleccionado no orientado a conexión.
5. *No repudio.*
   - Con prueba de origen.
   - Con prueba de destino.

De manera general se hará por el momento una breve descripción de cada servicio.

El servicio de *autenticación* involucra un requerimiento de identidad corroborable y distingue entre la *autenticación* de las partes que se comunican entre sí y la *autenticación* del origen de los datos.

El *control de acceso* es un servicio que proporciona protección a los recursos del sistema contra acceso y uso no autorizado. Este servicio esta íntimamente relacionado al de *autenticación* debido a que un usuario o proceso debe ser autenticado antes de tener acceso a cualquier recurso del sistema.

La *confidencialidad* también conocida como *privacidad* o privacía proporciona a los datos protección contra lectura o divulgación no autorizada. Este servicio oculta o transforma los datos de tal manera que solo las partes autorizadas puedan enterarse de su contenido.

El servicio de *integridad* protege a los datos contra modificaciones, alteraciones, borrado, inserciones, y de todo tipo de acción que atente contra su *integridad*.

El *no repudio* proporciona protección contra la posibilidad de que alguna de las partes involucradas en una comunicación nieguen ya sea haber enviado un mensaje u originado una acción, o bien nieguen haber recibido un mensaje o haber sido el destinatario de cierta acción.

La finalidad de este trabajo es establecer claramente todos los posibles riesgos que existen en un centro de cómputo, analizar las *vulnerabilidades* computacionales, e indicar que *servicio de seguridad* se podría asociar para proporcionar una recomendación que pudiese disminuirlos considerablemente.

Por todo lo antes mencionado se ha nombrado a este trabajo como: "*Análisis de riesgos* en centros de cómputo". El tipo de análisis de riesgo no será de índole financiera sino más bien de índole operativa - funcional.

Siempre que ha sido posible, se han añadido algunos localizadores de recursos uniformes (URL's) como referencias. Los URL's apuntan a los correspondientes documentos informativos en internet. Con respecto a dichos URL's se piden disculpas por aquellos que hayan podido desaparecer o hayan sido modificadas desde que se accesaron para tomar una idea complementaria a este trabajo.

1.2 Identificación del problema.

El cómputo cada día va asumiendo nuevas responsabilidades en las actividades ordinarias. Todo tipo de empresa sin importar su tamaño utiliza computadoras para organizar y controlar sus activos, nóminas y/o inventarios. El día de hoy se comienza a

dar la convergencia entre el comercio electrónico con las actividades cotidianas de muchas personas. Se comienza a dar un nuevo giro a los paradigmas de negocios cambiando la visión "business to costumer" por "business to business"

Es un hecho, la sociedad cada vez se vuelve más dependiente de la tecnología de la Información y del procesamiento automatizado de la misma, el no estar consciente de los riesgos que puedan afectar el funcionamiento normal del flujo de información en toda organización podría ocasionar un paro de actividades que se traduciría en atrasos con la producción de bienes y servicios.

Sin restarle importancia al tipo de procesador o a la velocidad de procesamiento o a la cantidad de memoria instalada o a cualquier periférico que una computadora tenga lo que la hace realmente vital y por lo tanto significativa, es la información que contiene, procesa, genera y/o transmite.

Cada centro de cómputo debe instrumentar las medidas que crea necesarias para proteger la información que utiliza, pero saber qué nivel de confianza posee sin recurrir a estudios serios constituiría una acción poco aplaudida y hasta cierto sentido la administración de los activos estaría sostenida por decisiones empíricas. Precisamente este trabajo intenta ser una guía para aquellos tomadores de decisiones al respecto y dar a conocer los *servicios de seguridad* existentes y que podrían disminuir la probabilidad de ocurrencia de los riesgos existentes en su centro de cómputo.

Actualmente los instrumentos de referencia en seguridad computacional son documentos provenientes de organizaciones de los Estados Unidos. Algunos de los centros especializados en materia de seguridad que de alguna manera tienen influencia en nuestro País son:

- El National Computer Security Center (NCSC quien publicó el libro de certificación conocido como "*Orange book*").
- El Computer Emergency Response Team (CERT), quien cuenta en México con un equipo de trabajo investigador de riesgos en cómputo de programas y productos comerciales. El CERT hace del conocimiento público las *vulnerabilidades* de todos los softwares comerciales pero hasta que encuentra la manera de evitar daños es entonces cuando da a conocer las *vulnerabilidades* acompañadas de su(s) solución(es). El CERT mexicano es conocido como Mx-CERT pero generalmente sólo se limita a hacer algunas traducciones de los documentos publicados por el CERT.
- El Computer Incident Advisory Capability.
- Publicaciones "Trusted Network Technology" especializadas en seguridad de redes de computadoras.

En México no se cuenta con alguna institución que certifique la seguridad de todas las actividades relacionadas con el tratamiento de la información, tampoco hay un documento oficial mexicano que se pueda utilizar como base para medir el grado de seguridad con que cuente un centro de cómputo en cuanto al manejo de información,

existe únicamente la voluntad por parte del INEGI[6] pero ninguna ley, decreto, reglamento o norma realizado al respecto. Lo que se da en este momento son acciones de control como auditorias y difusión de realización de respaldos por parte de alguna secretaría de estado (como SECODAM).

En realidad hay una escasez de proveedores de bienes y servicios relacionados con la seguridad de la información. Siendo reiterativos hasta el día de hoy no existe públicamente una empresa certificadora de seguridad, las empresas que existen son despachos particulares de consultores en seguridad como "Coopers and Lybrand S.A. de C.V."; "Cauferrat Consultores" y "SeguriDATA".

En la Universidad Nacional Autónoma de México se cuenta con dos organismos que laboran en el estudio de riesgos en materia de cómputo:

- El ASC, Área de Seguridad en Cómputo de la *D.G.S.C.A.*, y
- GASU, Grupo de Administradores en Sistemas *Unix*).

La seguridad en un centro de cómputo desde el punto de vista operacional, se ve comprometida de la siguiente manera, una persona que intenta entrometerse a un sistema (o incluso al propio *site*) persigue ciertos objetivos y para alcanzarlos se vale de ciertas herramientas para obtener un acceso. Obteniendo este acceso entonces actuará de alguna manera, obtendrá un resultado.

Atacantes → herramientas → Acceso → Resultados → Objetivos

El propósito final de un *análisis de riesgos* es ayudar a planear una protección efectiva justificable en costo que reduzca la probabilidad del riesgo hasta un nivel aceptable, en este caso la protección efectiva será uno de los *servicios de seguridad* mencionados en el apartado denominado "antecedentes".

El *análisis de riesgos* que se pretende realizar en este trabajo asume que el factor humano es la entidad potencial generadora de un riesgo y la computadora y su contenido (datos e información) son las víctimas cuando estas son vulnerables.

Una *vulnerabilidad* va acompañada de un riesgo, así la amenaza de fuego (riesgo de incendio) esta asociado con la *vulnerabilidad* de tener una inadecuada protección contra el fuego. La amenaza de accesos no autorizados esta íntimamente ligada a un inadecuado *control de acceso*. El riesgo de pérdida de datos críticos demuestra un deficiente o inexistente plan de contingencias.

[6] Información obtenida de una plática sostenida con la Dra. Lucia Andrade y el Lic. Ramón Ocampo del INEGI.

1.3 Demarcación del fenómeno (marco de referencia).

Todos los centros de cómputo independientemente del tipo de información que capten, procesen, desplieguen, distribuyan y/o almacenen tienen riesgos que son susceptibles de ser analizados.

De manera específica, hay 2 centros de cómputo en los que el responsable de este trabajo tiene acceso y permisos autorizados para desarrollar las actividades que sean necesarias, uno de ellos es el centro de cómputo de la Dirección de Cómputo para la Administración Académica (*D.C.A.A.*) y el segundo es el centro de cómputo del área de prospección e innovación de la *D.G.S.C.A.* Se tomarán escenarios de estos dos centros de cómputo para realizar el *análisis de riesgos*. Cabe señalar que este trabajo se desarrollará de manera general.

Se presenta a continuación una breve semblanza sobre las actividades que cubren tanto la *D.C.A.A.* como el área de prospección e innovación de la *D.G.S.C.A.*[7] y el papel que han de cubrir desde el año 2000.

La Dirección de Cómputo para la Administración Académica es un centro de excelencia en el desarrollo de sistemas para la Universidad. Al serlo cumple con su función de asesoría a las dependencias universitarias, ya sea que éstas realicen o que comisionen a terceros sus propios desarrollos.

A partir de 1997 la *D.C.A.A.* ha recibido el encargo de contemplar simultáneamente los desarrollos de sistemas basados en el manejo de grandes volúmenes de datos y aquellos en el que el acceso a los sistemas se basa en modelos y estándares similares a los de Internet. Se unen a esta Dirección las unidades dedicadas a la prestación de servicios basados en redes, ubicadas en la Dirección de Telecomunicaciones Digitales. Se refleja así la fusión de las diversas tecnologías de cómputo y telecomunicaciones.

La *D.C.A.A.* realiza estudios de reingeniería asociada a la introducción de los sistemas y experimentación con hardware y software para soluciones económicas y poderosas en su campo de acción. Presta servicios internos y externos de importancia, como los de impresión masiva y la producción de diversos medios de distribución de información.

Adicionalmente, la *D.C.A.A.* cumple para la Universidad funciones importantes que le son asignadas por la Dirección General, delegadas a ésta por el Consejo Asesor de Cómputo. Entre ellas destacan el análisis y control de las adquisiciones especiales de equipo de cómputo (mediante el trámite de "aval técnico"), el análisis y apertura de las ofertas de servicios de mantenimiento en el tránsito a la descentralización de la partida

[7] http://exodus.dcaa.unam.mx y http://www.dci.unam.mx

presupuestal correspondiente, y el análisis, negociación y contratación de licencias de software para la institución. Se promueve una acción intensificada en todas esas áreas.

El área de prospección e innovación de la *D.G.S.C.A.* tiene como propósito detectar los esquemas de aplicación de las tecnologías emergentes en la UNAM que puedan resultar de mayor utilidad a las actividades fundamentales de la propia Universidad y de la comunidad.

1.4 Conocimiento empírico en el medio.

Dentro del marco problemático se debe realizar una recopilación de distintos puntos de vista de personas directamente relacionadas en el medio de estudio con la finalidad de percibir en su opinión si existe un problema tal como se ha planteado hasta este momento, es decir, la finalidad que existe detrás de este tópico es percibir si las personas desde su perspectiva particular consideran útil o no el que se realicen estudios a los riesgos que afectan la información.

Para este efecto se hace distinción entre los tipos de personas a entrevistar:

- Personas sin perfil académico en cómputo que realizan actividades en cómputo (realmente son bastantes y no es nada raro en los centros de cómputo de la UNAM por ejemplo).
- Personas con perfil académico en cómputo que realizan actividades en cómputo pero no en cuestiones de seguridad.
- Personas con perfil académico en cómputo (profesionales) que se dedican al estudio o a la implantación de seguridad o a realizar *análisis de riesgos* en cómputo.

Estos tres grupos de personas laboran en los dos centros de cómputo mencionados en "Demarcación del fenómeno" aunque se debe mencionar que también se hará uso de internet para pedir opiniones de otras personas que se encuentren físicamente lejos de donde el autor pueda trasladarse con facilidad.

Los dos primeros tipos de personas se podría decir que tienen conocimientos prácticos o teóricos; el último tipo de personas corresponde al de profesionales en el medio, de las cuales se habla más en el punto 1.5.

Las opiniones serán recopiladas por medio de las técnicas de entrevista y/o cuestionario. Se aplicará el mismo cuestionario a los tres grupos de personas.

Enseguida se muestra el diseño de las preguntas, su justificación y la respuesta esperada, el formato del cuestionario se encuentra en el Anexo I -1.

Pregunta No. 1.
¿Usted cree conveniente el que se estudien los riesgos y las *vulnerabilidades* que afectan a la información que existe en un centro de cómputo?
Justificación: Esta pregunta permite obtener respuestas con mucha importancia ya que mostraría si el cuestionado considera a la información como un bien importante, de ahí que deba estudiarse, o tal vez mencione que no implica mayor importancia en su ámbito en cuyo caso se podría deducir que el activo más importante no tiene la importancia que debería poseer.
Respuesta esperada: Sí.

Pregunta No 2.
Mencione algunas ventajas y/o desventajas que usted conoce que pueden derivar de realizar un *análisis de riesgos*?
Justificación: Permite conocer si el cuestionado conoce la técnica de "*análisis de riesgos*".
Respuesta esperada: Varía.

Pregunta No. 3.
¿Usted cree que los datos que introduce en un sistema o que la información que obtiene de ellos esta segura?
Justificación: Permite conocer hasta qué grado una persona, usuario de sistemas y hasta diseñadores de los mismos (cuestionados) confían en los sistemas de información que utilizan.
Respuesta esperada: Sí.

Pregunta No. 4.
¿Sabe que es un *servicio de seguridad*?, si su respuesta es afirmativa por favor mencione su concepto.
Justificación: Permite saber hasta que grado de profundidad el cuestionado esta inmerso en el tema.
Respuesta esperada: varía.

Pregunta No. 5.
A su criterio cuáles deberían de ser los adjetivos asociados a la información para que ésta fuese aceptada por usted para realizar su trabajo. Indique por favor su área de trabajo: (administrativa, diseño gráfico, análisis, diseño de sistemas, programación, Tomador de decisiones, conectividad, otra).
Justificación: Esta pregunta va muy de la mano con la anterior ya que es muy probable que la respuesta que se dé se asocie con los *servicios de seguridad* de la pregunta anterior.
Respuesta esperada: Sí.

Pregunta No. 6.
¿Usted conoce, sabe o utiliza algún método para brindar seguridad a su información cotidiana tal como passwords, *cifrado* de información, respaldos, auditorías, etc.?
Justificación: Esta pregunta permite conocer si en el centro de cómputo se cuenta con algún plan de seguridad que trate de proteger a la información. Podríamos observar tal vez

que sólo un grupo de personas utilizan ciertos *servicios de seguridad* mientras otros no lo hacen (tal vez por ignorancia), hablaríamos entonces de grupos privilegiados y de grupos muy vulnerables.
Por lo general, la toma de conciencia acerca de la seguridad comienza con la preocupación de la alta dirección, el desarrollo de planes de seguridad, la implementación y por último la difusión masiva hacia el personal del estudio realizado y de las recomendaciones derivadas de él.
Respuesta esperada: Sí.

Pregunta No. 7.
¿La información sensible (indispensable) tiene alguna protección?
Justificación: Imagínese el escenario en el que un usuario autorizado con malas intenciones logre ganar el acceso a un archivo con información sensible. Si el archivo se protege (por ejemplo) cifrándolo, se puede asegurar la *confidencialidad* de la información. Sin embargo si ésta persona realmente tiene malas intenciones puede destruir el archivo *cifrado* almacenado en cuyo caso quizá el mejor remedio hubiese sido contar con un respaldo. Ahora, si los almacenamientos no son *cifrados*, incluso podría verse afectada la *integridad* de la información si se realiza un respaldo secundario con datos manipulados.
Respuesta esperada: No.

Pregunta No. 8.
¿En el área o centro de cómputo en donde usted labora, se cuenta con algún plan que proteja las transmisiones (telecomunicaciones)?
Justificación. Hasta el momento se han planteado riesgos que se generan en el centro de cómputo, sin embargo existen riesgos que pueden provenir de lugares remotos en los que hay que cuidar las líneas de transmisión, los puertos dial-up, incluso cuestionarse sobre la autenticidad de la parte remota. Si no hay ningún tipo de protección en este sentido entonces quizá ya se hayan generado *ataques* a la *confidencialidad, integridad* y/o disponibilidad de la información.
Respuesta esperada: Sí.

Pregunta No. 9.
¿Y con planes de recuperación de información?
Considerando respaldos, pérdidas o recuperación a intervenciones ilícitas.
Justificación: Una Ley de Murphy menciona que todos lo que puede fallar falla, siendo así podrían fallar los medios de almacenamiento o de procesamiento, por lo tanto es necesario contar con un plan de recuperación inmediata de información por medio de los respaldos y de algunas otras consideraciones de pérdida de información. El no contar con planes de recuperación de información puede afectar la disponibilidad de los servicios y la productividad de los usuarios.
Respuesta esperada: Sí.

Pregunta No. 10.
¿Se realizan pruebas de detección de passwords en los sistemas de *autenticación* multiusuarios para accesos locales y remotos?
Justificación: Si se utiliza Novel Netware V2.2 o V3.11 se puede saber cuántos usuarios no requieren passwords o cuántas cuentas de supervisor existen. Para el caso de Windows NT internet esta llena de programas de adivinación de passwords. En sistemas *UNIX* hay programas que utilizan la técnica de búsqueda por diccionario para encontrar posibles passwords con un alto porcentaje de aciertos[8]. Con una sola cuenta que sea penetrada por una persona distinta al dueño puede ocasionar varios destrozos al usuario suplantado o a algunas partes del sistema y/o afectando algunos *servicios de seguridad*. Si un intruso se encuentra en un sistema es muy posible que se haya atacado la *confidencialidad* de la información. Otros servicios afectados: *Integridad* y disponibilidad. Afectaciones en los recursos del sistema.
Respuesta esperada: Sí. Es muy común la información sobre éste problema ya que es muy frecuente.

El formato del cuestionario puede obtenerse en el Anexo I - 1.

1.5 Opiniones profesionales.

Como se ha mencionado en el punto anterior para los fines de este trabajo va a existir dentro del espacio muestral una distinción entre los tipos de personas a entrevistar. Una de estas distinciones es precisamente el perfil académico en cómputo y que además se dedican al estudio o a la implantación de mecanismos de seguridad o a realizar *análisis de riesgos* en cómputo.

- Personas que laboren en el ASC (Área de Seguridad en Cómputo de la *D.G.S.C.A.*)
- Personas que laboren en el grupo de seguridad de la *D.C.A.A.*
- *Hackers.*

Breve semblanza Histórica del Área de Seguridad en Cómputo de la *D.G.S.C.A.*: [9]

Desde la compra de la supercomputadora Cray YMP 4/464 en el año de 1991, el Departamento de Supercómputo de la *D.G.S.C.A.* se preocupó por la seguridad, tanto de la super computadora, como del resto de las máquinas del departamento.

[8] Algunas pruebas han *descifrado* hasta en un 25 % el total de passwords obteniendo la palabra o palabras secretas en claro.
[9] Obtenida del URL http://www.asc.unam.mx

El número de máquinas del departamento fue creciendo, así como las actividades requeridas para poder mantener un buen nivel de seguridad en ellas. Por otro lado, cada vez se tenía más información de problemas de seguridad en la UNAM y en el resto del mundo. Dada la importancia y naturaleza de estos problemas, surgió la idea de formar un Área dedicada a la seguridad en cómputo, cuyo rango de acción no se limitara al Departamento de super cómputo, sino que atendiera las necesidades de la UNAM y difundiera a nivel nacional e internacional la cultura de la seguridad en cómputo.

Esta idea fue apoyada por la entonces Jefa del Departamento de Super cómputo Lic. Martha Sánchez y por los directores de la Dirección para la Investigación Dr. Alonso y de la *D.G.S.C.A.* Dr. Victor Guerra.

En Agosto de 1995, se formó de manera oficial, lo que en aquel entonces fue llamado, el ESC (Equipo de Seguridad en Cómputo) dirigido por el Ing. Diego Zamboni, quien había trabajado anteriormente en cuestiones de seguridad para el departamento de super cómputo y presentado, para obtener su título de Ingeniero, la tesis "Proyecto UNAM/Cray de Seguridad en el Sistema Operativo *UNIX* que involucra la formación de un grupo independiente para atender las necesidades de seguridad.

En su propuesta original el ESC perseguía los siguientes objetivos:

- Difundir información sobre seguridad en cómputo.
- Crear y difundir políticas de seguridad en cómputo.
- Ofrecer *servicios de seguridad* en cómputo.
- Ofrecer un servicio especial de respuesta a incidentes
- Crear, capacitar y promover grupos humanos dedicados a la seguridad en cómputo.
- Realizar investigación y desarrollo sobre seguridad en cómputo.

Debido a la labor tan importante que desempeñaba el ESC, sus actividades encaminadas a promover la cultura de la Seguridad en Cómputo aumentaron, por lo que se convirtió en el Área de Seguridad en Cómputo (ASC).

Del ASC también se han obtenido algunas respuestas al cuestionario mencionado con anterioridad, enseguida se nombran las personas a quienes han colaborado y que corresponden a profesionales en temas de seguridad:

Iliana Meneses Hernández
ASC DCI *D.G.S.C.A.* UNAM *Ciudad universitaria*
Administradora de Seguridad de Sistemas *Unix*.

Marcos Iván Hernández Pérez.
D.C.A.A.-D.G.S.C.A.
Encargado de la administración y seguridad de Sistemas *UNIX*.

Gunnar Wolf
ASC DCI *D.G.S.C.A.* UNAM ENEP Iztacala.
Jefe de Sección de Administración. de Sistemas y Telecomunicaciones

Germán Santos Jaimes
D.G.S.C.A.
Administrador de Servidores. Actualmente imparte clases de Seguridad e intrusiones en sistemas *UNIX* en la Facultad de Ingeniería en C.U.

"KCool"
Hacker. Su dominio se encuentra dentro de la UNAM y se puede visitar su página de web en la siguiente dirección:
http://bufadora.astrosen.unam.mx/~desi/*hacker*.html

Los resultados de las encuestas se pueden encontrar en el anexo I-4

1.6 Hipótesis preliminar.

Presentación del problema en su relación causa - efecto.

CAUSA (Variable independiente)	EFECTOS (Variables dependientes)
• Si un centro de cómputo realiza un análisis de los riesgos que afectan a la información que captan, procesan, despliegan, distribuyen y/o almacenan.	• se puede crear un plan de reducción de riesgos con objetividad. • se pueden determinar algunas necesidades no detectadas en la empresa. • se pueden cuantificar los riesgos a los cuales están sujetos los activos. • se puede estimar la probabilidad de ocurrencia de cada riesgo latente. • se pueden revisar y redefinir los controles de seguridad ya existentes. • se pueden asignar para su estudio pocos recursos tanto humanos, financieros y/o materiales. • Se pueden conocer los *servicios de seguridad* con que cuentan los procesos que la utilicen (a la información). • se pueden establecer bases para una toma de decisiones.

Relaciones hipotéticas posibles:

A) En forma positiva:

- Si un centro de cómputo realiza análisis de los riesgos que afectan a la información que captan, procesan, despliegan, distribuyen y/o almacenan entonces se puede crear un plan de reducción de riesgos con objetividad.

- Si un centro de cómputo realiza análisis de los riesgos que afectan a la información que captan, procesan, despliegan, distribuyen y/o almacenan entonces se pueden determinar algunas necesidades no detectadas en la empresa.
- Si un centro de cómputo realiza análisis de los riesgos que afectan a la información que captan, procesan, despliegan, distribuyen y/o almacenan entonces se pueden cuantificar los riesgos a los cuales están sujetos los activos.
- Si un centro de cómputo realiza análisis de los riesgos que afectan a la información que captan, procesan, despliegan, distribuyen y/o almacenan entonces se puede estimar la probabilidad de ocurrencia de cada riesgo latente.
- Si un centro de cómputo realiza análisis de los riesgos que afectan a la información que captan, procesan, despliegan, distribuyen y/o almacenan entonces se pueden revisar y redefinirse los controles de seguridad ya existentes.
- Si un centro de cómputo realiza análisis de los riesgos que afectan a la información que captan, procesan, despliegan, distribuyen y/o almacenan entonces se pueden asignar para su estudio pocos recursos tanto humanos, financieros y/o materiales.
- Si un centro de cómputo realiza análisis de los riesgos que afectan a la información que captan, procesan, despliegan, distribuyen y/o almacenan entonces se pueden conocer los *servicios de seguridad* con que cuentan los procesos que la utilicen (a la información).
- Si un centro de cómputo realiza análisis de los riesgos que afectan a la información que captan, procesan, despliegan, distribuyen y/o almacenan entonces se pueden establecer bases para una toma de decisiones.

B) En forma negativa:

- Si un centro de cómputo no realiza análisis de los riesgos que afectan a la información que captan, procesan, despliegan, distribuyen y/o almacenan entonces no se puede crear un plan de reducción de riesgos con objetividad.
- Si un centro de cómputo no realiza análisis de los riesgos que afectan a la información que captan, procesan, despliegan, distribuyen y/o almacenan entonces no se pueden determinar algunas necesidades no detectadas en la empresa.
- Si un centro de cómputo no realiza análisis de los riesgos que afectan a la información que captan, procesan, despliegan, distribuyen y/o almacenan entonces no se pueden cuantificar los riesgos a los cuales están sujetos los activos.
- Si un centro de cómputo no realiza análisis de los riesgos que afectan a la información que captan, procesan, despliegan, distribuyen y/o almacenan entonces no se puede estimar la probabilidad de ocurrencia de cada riesgo latente.
- Si un centro de cómputo no realiza análisis de los riesgos que afectan a la información que captan, procesan, despliegan, distribuyen y/o almacenan entonces no se pueden revisar y redefinirse los controles de seguridad ya existentes.

- Si un centro de cómputo no realiza análisis de los riesgos que afectan a la información que captan, procesan, despliegan, distribuyen y/o almacenan entonces no se pueden asignar para su estudio pocos recursos tanto humanos, financieros y/o materiales.
- Si un centro de cómputo no realiza análisis de los riesgos que afectan a la información que captan, procesan, despliegan, distribuyen y/o almacenan entonces no se pueden conocer los *servicios de seguridad* con que cuentan los procesos que la utilicen (a la información).
- Si un centro de cómputo no realiza análisis de los riesgos que afectan a la información que captan, procesan, despliegan, distribuyen y/o almacenan entonces no se pueden establecer bases para una toma de decisiones.

Las relaciones hipotéticas en su forma negativa no deforman los efectos de las relaciones hipotéticas posibles en su forma positiva.

C) Hipótesis propuesta.

Si un centro de cómputo realiza análisis de los riesgos que afectan a la información que captan, procesan, despliegan, distribuyen y/o almacenan entonces se pueden crear planes de reducción de riesgos objetivos, se pueden determinar algunas necesidades no detectadas en la empresa, se pueden cuantificar los riegos a los cuales están sujetos los activos, se puede estimar la probabilidad de ocurrencia de cada riesgo latente, se pueden revisar y redefinir los controles de seguridad ya existentes, se pueden asignar para su estudio pocos recursos tanto humanos, financieros y/o materiales, se pueden conocer los *servicios de seguridad* con que cuentan los procesos que la utilicen (a la información) y se pueden establecer bases para una toma de decisiones.

1.7 Objetivos (marco justificatorio).

A) Personales:

- Obtener el título profesional de la licenciatura en informática en la Facultad de Contaduría y Administración de acuerdo con las disposiciones oficiales en los artículos 18, 19 y 20 del Reglamento General de Exámenes vigente[10] y en las disposiciones oficiales de los artículos 3, 7e), 9g) y 44 al 55 del Nuevo Reglamento de Exámenes Profesionales vigente. [11]

[10] En el anexo I-2 se hace una réplica textual de los artículos referidos.
[11] En el anexo I-3 se hace una réplica textual de los artículos referidos.

- Difundir la necesidad de realizar estudios de éste tipo.

- Corresponder tanto a la Dirección de Cómputo para la Administración Académica *D.C.A.A.* como a la Subdirección de cómputo para la Investigación de la *D.G.S.C.A.*, con éste trabajo por la valiosa parte de mi formación profesional obtenida en ambas dependencias.

- Proporcionar un instrumento de apoyo para estudios posteriores.

B) Particular:

- Aplicar una metodología de *análisis de riesgos* que pueda ser tomada como guía de protección a los activos en cualquier centro de cómputo.

1.8 Conclusiones al primer capítulo.

En este capítulo se presentó una perspectiva histórica relacionada al desarrollo que ha tenido el tópico de seguridad computacional en nuestro país. Realmente todo ambiente de inseguridad es dado por el factor humano (excluyendo algunos ambientes geológicos claro).

Se ha hablado de la arquitectura de seguridad del *modelo OSI* y de los cinco *servicios de seguridad* definidos en ella.

Se ha hecho mención de la dependencia actual de la tecnología de información. El pasar por alto todos los riesgos que puedan afectar a la información tratada ocasionará que si se hace presente un factor de riesgo, la pérdida por asumir la falta puede ser muy elevada (y en ocasiones no bastará con reponer lo perdido –que en ocasiones no podrá ni siquiera poder reponerse-).

Se ha hecho notoria la escasa atención que las autoridades mexicanas han hecho al respecto y se han mencionado algunas entidades que se hacen cargo actualmente de la administración de los riesgos computacionales en nuestro País.

Se han establecido los distintos puntos de vista de personas que trabajan en actividades relacionadas al cómputo y se les ha aplicado un cuestionario. Los resultados de esta primer aproximación arrojan que si tienen presentes algunas *vulnerabilidades* de las herramientas con las que todos los días captan, procesan, despliegan y/o distribuyen, sin embargo esa información que tienen posiblemente no sea suficiente como para poder establece medidas de prevención y recuperación ante un siniestro que se genere. Esto precisamente constituye material suficiente para establecer una hipótesis preliminar de trabajo.

1.9 Anexos.

Anexo I – 1.

Cuestionario

El objetivo de este cuestionario es conocer su opinión respecto al tema de ***análisis de riesgos*** en la información que utiliza usted todos los días en su centro de trabajo. Por favor trate de ser extenso en sus respuestas.
Algunas preguntas contienen algunos conceptos implícitos.

1. ¿Usted cree conveniente el que se estudien los riesgos y las ***vulnerabilidades*** que afectan a la información que existe en un centro de cómputo?

___ Sí, ¿por qué? _____

___ No, ¿por qué? _____

___ otra respuesta.
¿cuál? _____

2. Mencione algunas ventajas y/o desventajas que usted conoce que pueden derivar de realizar un ***análisis de riesgos***?

Ventajas (beneficios)	Desventajas (males)

3. ¿Usted cree que los datos que introduce en un sistema o que la información que obtiene de ellos esta segura?

___ Sí, ¿por qué? _____

___ No, ¿por qué? _____

___ otra respuesta. ¿cuál? _____

4. ¿Sabe que es un *servicio de seguridad*?, si su respuesta es afirmativa por favor mencione su concepto.

___Sí, _____

___ No
___ otra respuesta. ¿cuál?_____

5. A su criterio cuáles deberían de ser los adjetivos asociados a la información para que ésta fuese aceptada por usted para realizar su trabajo. Indique por favor su área de trabajo:

___ Administrativa ___ Diseño gráfico ___ Análisis
___ Diseño de sistemas ___ programación ___ Tomador de decisiones
___conectividad ___ otra

La información_____

6. ¿Usted conoce, sabe o utiliza algún método para brindar seguridad a su información cotidiana tal como password, *offsite* de información, respaldos, auditorías, etc.?

___ Sí, ¿cuáles? _____

___ No
___ otra respuesta. ¿cuál?_____

7. ¿La información sensible (indispensable) tiene alguna protección?

___ Sí, ¿por qué? _____

___ No, ¿por qué? _____

___ otra respuesta. ¿cuál?_____

8. ¿En el área o centro de cómputo en donde usted labora, se cuenta con algún plan que proteja las transmisiones (telecomunicaciones)?

___ Sí, ¿por qué? _____

___ No, ¿por qué? _____

___ otra respuesta. ¿cuál? _____

9. ¿Y con planes de recuperación de información?
Considerando respaldos, pérdidas o recuperación a intervenciones ilícitas.

___ Sí, ¿cuáles? _____

___ No, ¿por qué? _____

___ otra respuesta. ¿cuál? _____

10. ¿Se realizan pruebas de detección de passwords en los sistemas de ***autenticación*** multiusuarios para accesos locales y remotos?

___ Sí, ¿por qué? _____

___ No, ¿por qué? _____

___ otra respuesta. ¿cuál? _____

Anexo I-2

Reglamento general de exámenes 1997.

CAPÍTULO IV

Exámenes profesionales y de Grado.

Artículo 18.- Los objetivos de los exámenes profesionales y de grado son: valorar en conjunto los conocimientos generales del sustentante en su carrera o especialidad; que éste demuestre su capacidad para aplicar los conocimientos adquiridos y que posee criterio profesional.

Artículo 19.- (Modificado en la sesión del Consejo Universitario del 9 de noviembre de 1978, como sigue):

Artículo 19.- En el nivel de licenciatura, el título se expedirá, a petición del interesado, cuando haya cubierto el plan de estudios respectivo y haya sido aprobado en el examen profesional correspondiente. El examen profesional comprenderá una prueba escrita y una oral. Los consejos técnicos de las facultades o escuelas podrán resolver que la prueba oral se sustituya por otra prueba escrita. Cuando la índole de la carrera lo amerite habrá, además, una prueba práctica.

Artículo 20.- La prueba escrita podrá ser una tesis o, en los casos establecidos por el consejo técnico correspondiente:

a) Un trabajo elaborado en un seminario, laboratorio o taller, que forme parte del plan de estudios respectivo;
b) Un informe satisfactorio sobre el servicio social, si éste se realiza después de que el alumno haya acreditado todas las asignaturas de la carrera correspondiente, y si implica la práctica profesional.

Anexo I-3

Nuevo Reglamento de Exámenes Profesionales aprobado por el Consejo Técnico de la Facultad de Contaduría y Administración, el 29 de abril de 1999.

TÍTULO I
Generalidades.

Artículo 3. Para obtener el título de Licenciado en Contaduría, en Administración o en Informática se requiere aprobar el examen profesional correspondiente, que comprenderá una prueba escrita y oral.

TÍTULO II
De la prueba escrita.

Artículo 7. La prueba escrita del examen profesional, podrá realizarse de conformidad con las siguientes opciones:

e) Elaborar una tesis profesional.

Artículo 9. Para la realización de la prueba escrita, debe elegirse una de las siguientes áreas de conocimiento establecidas en los planes de estudio de las licenciaturas que se imparten en la Facultad:

g) Informática.

Artículo 44. Esta opción tiene como objetivo contribuir tanto a la formación metodológica del alumno como al avance de la investigación en las disciplinas propias de la Facultad, mediante la realización de una tesis por el estudiante bajo la dirección de un profesor que reúna los requisitos del artículo 51. La tesis consistirá en una investigación básica o aplicada en la que el alumno plantee y busque la solución de un problema del campo de alguna de las disciplinas de la Facultad.

Artículo 45. La tesis que elabore el alumno deberá ser afín a una de las líneas de investigación que se estén desarrollando en la Facultad.

Artículo 46. Para poder elaborar su tesis el alumno deberá inscribirse a un seminario de investigación de alguna de las áreas de conocimiento de su carrera que señala el artículo 9, de conformidad con su tema de investigación. En dicho seminario un profesor le dirigirá su trabajo.

Artículo 47. El seminario de investigación tendrá una duración de un semestre, que podrá ser prorrogado por un semestre más mediante la reinscripción correspondiente.

Artículo 48. El alumno podrá inscribirse al seminario de investigación a partir del último semestre del plan de estudios de su carrera.

Artículo 49. Para inscribirse a un seminario de investigación el alumno deberá cubrir los siguientes requisitos:

a) Haber acreditado todas las asignaturas previas al último semestre de su carrera.
b) Presentar su proyecto de investigación a un profesor del área de conocimiento afín al mismo, que cumpla además con los requisitos que señala el artículo 51 y obtener de él la aprobación escrita del proyecto, así como su aceptación para dirigirlo.

Artículo 50. El alumno deberá solicitar su inscripción al seminario de investigación ante la Coordinación de Exámenes Profesionales y Obtención de Grados Académicos de la Facultad, la cual extenderá, en su caso, la autorización correspondiente, misma que incluirá el nombre del profesor que deberá dirigirle la tesis.

Artículo 52. La tesis puede realizarse en cualquiera de las siguientes modalidades:

a) Individual o grupal unidisciplinaria: la que realicen uno o varios alumnos de la misma carrera.
b) Grupal interdisciplinaria: la que realicen varios alumnos de diversas carreras de las que se imparten en la Facultad.
c) Grupal multidisciplinaria: la que realicen varios alumnos de diversas carreras de las que se imparten en la UNAM, previa autorización de las facultades o escuelas involucradas.

Artículo 53. El número de alumnos que se reúnan para realizar una investigación grupal no podrá ser superior a tres. Cuando por excepción las investigaciones ameriten un número mayor, la autorización quedará a juicio del Consejo Técnico, previa fundamentación del director de la tesis quién tomará en consideración la extensión, grao de dificultad y alcance del trabajo.

Artículo 54. La prueba escrita del examen profesional mediante la opción de elaborar una tesis se acreditará con la aprobación escrita correspondiente emitida por el director del trabajo y la presentación impresa del mismo.

Artículo 55. Para efectos de la prueba oral del examen profesional, la tesis tendrá una vigencia de un año. Transcurrido este plazo el alumno deberá solicitar a la Coordinación de Exámenes Profesionales y Obtención de Grados Académicos que se le asigne un revisor de su trabajo de investigación, para que determine si éste requiere, por tratarse de un campo de desarrollo muy dinámico, alguna actualización. De ser así, el profesor orientará al alumno acerca de las modificaciones necesarias y, una vez que el alumno las realice, aprobará por escrito la actualización del trabajo.

Anexo I-4

Resultados de los cuestionarios aplicadas:

Lista de personas entrevistadas.

Tipo A: Personas sin perfil académico en cómputo que realizan actividades en cómputo:

Ivan Gabriel Figueroa Uribe (estudiante de la licenciatura en contaduría).
Se encargó de diversas actividades de cómputo en el Departamento de prospección e innovación de la *D.G.S.C.A.*
clave: E1_tipoA

Verena Gama Ugalde (estudiante de la licenciatura en contaduría).
Ha laborado por más de año y medio en el Departamento de Innovación tecnológica de la *D.C.A.A.*
clave: E2_tipoA

Irene Gabriela Sánchez González (estudiante de la licenciatura en contaduría).
Realiza actividades de auditoria y normatividad de sistemas de información dentro de la *D.C.A.A.*
clave: E3_tipoA

L.A. Roberto Víveros Fong Choi
Labora en el Departamento de Recursos Humanos y e imparte instrucción de algunos tópicos de computación.
clave: E4_tipoA

Actuario Ismael Carballo Sánchez.
Desarrollador de software en una consultoría de desarrollo de Software. Laboró en la misma actividad en la Coordinación de Prospección e innovación de la *D.G.S.C.A.*
Clave: E5_tipoA

Tipo B: Personas con perfil académico en cómputo que realizan actividades en cómputo pero no en cuestiones de seguridad.

Lic. Gerardo Martínez Gil
Gerente del Área de Desarrollo de Interware de México S.A. de C.V.
Premio Gabino Barreda.
clave: E1_tipoB

L.I. Hugo Alonso Reyes Herrera
Jefe del Departamento de integración de sistemas.
clave: E2_tipoB

Omar Vicencio Luna (estudiante de Ingeniería en comunicaciones).
becario de la *D.C.A.A.* Realiza actividades relacionadas con el equipo A12.
clave: E3_tipoB

Edgar Mendoza Arreola
Becario de la *D.C.A.A.* Realiza labores de programación.
Clave: E4_tipoB

Carlos Fernando Rey Trejo.
Consultor independiente.
Clave: E5_tipoB

Tipo C: Personas con perfil académico en cómputo (profesionales) que se dedican al estudio o la implementación de seguridad o a realizar *análisis de riesgos* en cómputo.

Iliana Meneses Hernández
Administradora de Seguridad de Sistemas *Unix*,
Clave: E1_tipoC

Marcos Iván Hernández Pérez.
Administración y seguridad de Sistemas *UNIX*
Clave: E2_tipoC

Gunnar Wolf
Jefe de Sección de Administración de Sistemas y Telecomunicaciones
Clave: E3_tipoC

Germán Santos Jaimes
Administrador de Servidores. Actualmente imparte clases de Seguridad e intrusiones en sistemas *UNIX* en la Facultad de Ingeniería en C.U.
Clave: E4_tipoC

"KCool"
Hacker de la facultad de ciencias en *Ciudad universitaria*.
Clave: E5_tipoC

A continuación se resumen y analizan las respuestas proporcionadas por las personas encuestadas:

1. ¿Usted cree conveniente el que se estudien los riesgos y las *vulnerabilidades* que afectan a la información que existe en un centro de cómputo?			
	☐ Sí, ¿por qué	☐ No, ¿por qué	☐ Otra respuesta. ¿Cuál?
E1_TipoA	Porque puede haber pérdidas de datos o infiltración de otras personas a información confidencial.		
E2_TipoA	Sí porque en cada área la información que se maneja es confidencial, y tanto el acceso a ella como el cuidado en su manejo y su almacenamiento es importante para la institución, por lo que hay que tomar en cuenta más de una alternativa.		
E3_TipoA	Sí. La información es materia prima de muchos de los procesos Involucrados en las organizaciones, principalmente aquellas que cuentan con un Centro de cómputo dedicado a tal tarea.		
E4_TipoA	Sí. Para adoptar medidas de mitigación de riesgos para cualquier tipo de desastres (naturales o causados por el hombre)		
E5_TipoA	Sí porque en una sala de cómputo entra mucha gente de las cuales algunas no saben utilizar la computadora y como consecuencia no sabe si su información puede ser afectada o puede afectar.		

E1_TipoB	Sí porque es importante analizar todos los factores de riesgo que involucra no solamente el equipo de cómputo y la información sino también su influencia en el ser humano.		
E2_TipoB	Si porque debido a que la información es precisamente el recurso más valioso de cualquier centro de cómputo. Un equipo se puede reemplazar, la información como tal a veces es imposible.		
E3_TipoB	Si, esto permitirá tener mejores sistemas de información con más seguridad.		
E4_TipoB	Si. Es un hecho que desde hace algunos años hasta nuestros días la información Se ha vuelto uno de los activos principales de toda empresa u organización. La información ahora representa una herramienta poderosa de mercado, política, financiera, etc. El problema es que no hay mucha gente especializada en la materia en nuestro país para lograr que el *análisis de riesgos* se vuelva una practica de trabajo cotidiana.		
E5_TipoB			Dependerá de lo valioso que representa para la organización el tener en un estado de *integridad*, confiabilidad, *privacidad*, etc. su información. Ejemplo trivial: Un banco lo tendrá que hacer, debido a la importancia económica que representa para este.
E1_TipoC	Sí porque se esta confiando la información a recursos que desde su diseño y en su uso presentan graves problemas de seguridad. La pérdida, alteración, borrado o divulgación de nuestra información podría causar que nuestra institución sufriera graves daños. El estudiar los riesgos nos permitirá desarrollar un esquema de seguridad para mitigarlos.		
E2_TipoC	Sí. Indispensable. La empresa que no lo hiciera así estaría condenada al fracaso.		
E3_TipoC	Sí. Ayuda a formar administradores y usuarios más conscientes y con mayor cultura informática.		
E4_TipoC	Si. Permite reducir el número de fallas en la organización.		

E5_TipoC	Si porque debemos conocer que debilidades existen en nuestro centro para poder siquiera conocer a que nos enfrentamos y posteriormente resolver dichos problemas.		

2) Mencione algunas ventajas y/o desventajas que usted conoce que pueden derivar de realizar un *análisis de riesgos*?		
	Ventajas (beneficios)	Desventajas (malos)
E1_TipoA	• Evitar pérdida de información. • Evitar *intrusos* en la información. • Identificar posibles fallas del sistema que identificaría pérdida de información. • Robustece los sistemas. • Se eliminarían ciertos *fugs*. • Beneficios a largo plazo.	• Muy caro al principio.
E2_TipoA	???	???
E3_TipoA	• Cualificar la información generada. • Determinación de la infraestructura básica para la seguridad de la información. • Planeación de contingencias y procedimientos alternos.	• Evidenciar los riesgos ante personas que puedan dañar a la institución. • Que sea utilizada para golpear políticamente al área de sistemas.
E4_TipoA	• Conocer mediante el BIA (Business Impact Analysis) las áreas que soportan la operación crítica de la empresa. • Definir las medidas de mitigación de riesgos para los procesos críticos del negocio, sin derivar esfuerzos en áreas que no lo son. • Tener conocimiento de aquellos tipos de riesgos que amenazan la • Operación modular del negocio. • Etc.	• Costo de inversión propios del análisis. • Inversión en medidas de mitigación de riesgos derivados del estudio • (equipamiento de un centro alterno, resguardo y respaldos de la información, etc.)
E5_TipoA	• Mayor seguridad en el manejo de la información.	• Las personas no estarían dispuestas a participar por flojera u otra cosa.
E1_TipoB	• Poder estimar costos de mantenimiento. • Poder evitar riesgos. • Controlar riesgos.	???
E2_TipoB	• Previsión de daños. • Conocimiento de posibles causas. • Preparación ante un problema. • Protección de los datos. • Seguridad en procesos. • Continuidad en operación.	• Tiempos. • Costos de procesos alternativos y de recuperación. • Costo en equipos de respaldo.
E3_TipoB	• Mayor confiabilidad.	• Mayores costos.
E4_TipoB	• La ventaja directa es la concientización sobre el valor de la información que derive en la implantación de determinadas políticas y mecanismos de protección de la misma.	• Los costos en que puede derivar dicho análisis, desde los costos por el servicio de análisis, como los costos involucrados en la implantación de los mecanismos de protección.

E5_TipoB	• Al realizar un *análisis de riesgos* se podrá establecer la protección del activo físico (computadoras, redes, el mismo edificio). • Se pueden determinar a partir de este análisis las políticas de seguridad de acceso al centro y/o al sistema(s) de información (bases de datos, respaldos, etc.). Y un montón de cosas más.	• Para aquellas organizaciones que no cuentan con los recursos humanos y monetarios representa claro una pérdida de tiempo y dinero que pueden ser utilizados para otros proyectos de mayor prioridad, con esto no quiero decir que este tipo de proyectos no sean importantes, sólo que muchas veces no tienen dentro de las organizaciones una importancia adecuada.
C1_TipoC	• Las ventajas que podemos obtener mediante la realización de un *análisis de riesgos* es principalmente poder ver las *vulnerabilidades* de nuestros equipos y nuestros sistemas de información, y de esa manera poner en práctica planes y políticas de seguridad, que ayuden a mantener a los sistemas lejos de los atacantes.	• La implantación de sistemas de seguridad puede ser costosa y será necesario actualizar los sistemas constantemente, ya que día tras día surgen nuevos *ataques* y se encuéntran hoyos de seguridad en los sistemas implantados. Es necesario tomar en cuenta que un sistema de seguridad no es 100% seguro, ya que se puede romper todo acceso mediante la técnica de fuerza bruta.
E2_TipoC	• Disminuir las *vulnerabilidades*. • Identificar amenazas potenciales. • Selección de herramientas para manejo de riesgos o de seguridad. • Protección de nuestros recursos. • Se adquiere un nivel de confianza mínimo requerido.	• Costos (sin embargo, la protección de los recursos es comúnmente más importante) y la pérdida de los mismos es frecuentemente más caro. • Es imposible eliminar por completo un riesgo. • Es difícil detectar algunos riesgos potenciales.
E3_TipoC	• Nos da mucho mayor conocimiento acerca de nuestra red y posibilidades de defendernos de posibles *ataques*.	• Requiere mucho tiempo hacerlo correctamente
E4_TipoC	• Permite optimizar Costos • Ayuda a que la duración de equipo sea adecuada.	• Necesita mucho tiempo.
E5_TipoC	• Mayor confiabilidad en mi información.	• Puede ser muy costoso. • Pérdida de tiempo.

3) ¿Usted cree que los datos que introduce en un sistema o que la información que obtiene de ellos esta segura?			
	☐ Sí, ¿por qué	☐ No, ¿por qué	☐ Otra respuesta. ¿Cuál?
E1_TipoA		No porque hay muchos factores que la pueden afectar y que pueden suceder cuando menos lo pensamos.	
E2_TipoA			Eso depende, del recurso humano por ejemplo, no sabes si alguien que tenga acceso a ella pueda filtrar información; por otra parte están los medios de almacenamiento y la

			cantidad de respal-dos que se hagan... por eso digo que es muy relativo.
E3_TipoA			Es segura en la medida que tal sistema cuente con la infraestructura de seguridad adecuada.
E4_TipoA			Depende en gran medida de la plataforma, diseño, construcción, etc. en el que este soportado.
E5_TipoA		No porque uno no sabe de donde proviene esa información.	
E1_TipoB		No porque en primera instancia el hardware es un factor de riesgo, en segundo lugar, no existe hasta la fecha un sistema totalmente seguro de donde obtener los datos o guardarlos.	
E2_TipoB		No porque es indispensable conocer el enfoque mismo del sistema, su interacción con otros sistemas, su conectividad, su seguridad contra violaciones, la corrupción de datos, etc..	
E3_TipoB		No porque todos los sistemas son vulnerables a alguna cosa, aunque las probabilidades actualmente son muy bajas de que pase algo inesperado.	
E4_TipoB			Todo depende del interés y nivel de preparación de la persona que interactúa con un sistema. El primer paso para confiar o desconfiar en las Respuestas de un sistema es la concientización acerca de lo importante que es la información generada o introducida al mismo, así como los riesgos para la persona misma, o bien la organización en que labora, si Es que existe un comportamiento anómalo. Después viene la capacitación sobre políticas y mecanismos que el usuario puede practicar para garantizar que su interacción con el sistema es confiable. Un ejemplo podría ser el uso de secure *shell* en sistemas *unix* para establecer sesiones remotas con un servidor.
E5_TipoB			Depende del sistema de que se esté hablando. En un cajero

			automático el NIP viaja seguro por la red, en un chat mi id, ip, y otras cosas pueden ser conocidos de forma relativamente fácil.
E1_TipoC			Todo depende de los sistemas de seguridad que sean implementados. Si el sistema no cuenta con algún mecanismo de defensa, es muy probable que la información que ingresa o sale de él pueda estar alterada o sea robada para fines distintos a los establecidos.
E2_TipoC		No, porque nuestra información tiene un nivel de protección a nivel de host y otro un poco menor a nivel de red.	
E3_TipoC			Depende del sistema, los datos, el mecanismo de introducción y el mecanismo de recuperación.
E4_TipoC		No. Existen muchísimos factores que me hacen pensar que no, además he vivido experiencias en carne viva que me han enseñado que siempre van a existir personas cuya idea diaria sea el penetrar un sistema.	
E5_TipoC		No porque siempre van a existir circunstancias que atenten contra la seguridad de la información (tales como crackers, hoyos de seguridad en el sistema, errores en la red incluso hasta desastres naturales.	

4. ¿Sabe que es un *servicio de seguridad*?, si su respuesta es afirmativa por favor mencione su concepto.			
Clave	☐ Sí	☐ No	☐ Otra respuesta. ¿Cuál?
E1_TipoA	Si. Es una estandarización que permite saber si una aplicación la cumple.		
E2_TipoA	Sí. Para mi un *servicio de seguridad* es una serie de métodos o Procedimientos que se cubren para proteger, en este caso, información. Debe tener sus políticas tanto de control como de acceso, acerca de la Periodicidad de acuerdo como lo demande el usuario.		
E3_TipoA	Si, Un conjunto de herramientas y técnicas que aseguran que los flujos de información y sus usuarios conserven la auntenticidad y *confidencialidad* de los datos.		

E4_TipoA	Sí, pero depende de que tipo y nivel de seguridad de la información se trate, por ejemplo: Seguridad de acceso por niveles de usuario, por sistema operativo, por programa, memí, base de datos, acceso al *site* de cómputo, comunicaciones, etc. En fin, la pregunta es muy abierta.		
E5_TipoA		No.	
E1_TipoB	Si, es un requerimiento fundamental para todo sistema privado o público que proclame ser más confiable que cualquier otro que no implemente un *servicio de seguridad.*		
E2_TipoB	Sí son servicios que permiten que la información sea manipulada por personas autorizadas y con la capacidad para hacerlo. Los *servicios de seguridad* permiten que los usuarios autorizados la puedan cambiar, quien tenga permiso consultarla, quien no, no la podría (ni debería conocer). Los *servicios de seguridad* proporcionan a la información confiabilidad y veracidad.		
E3_TipoB	Sí, los *servicios de seguridad* permiten que la información sea confidencial.		
E4_TipoB	Un servicio es toda acción tomada para producir un resultado o sensación de utilidad a la persona o entidad que lo solicita. Los *servicios de seguridad* son los mecanismos y acciones puestas en practica con el fin De brindar seguridad a ciertas entidades contra factores ajenos a su voluntad.		
E5_TipoB	Sí. Un *servicio de seguridad* en computo, es aquel que se encarga de establecer Los mecanismos necesarios para mantener la *integridad, confidencialidad* y *privacidad* de un sistema de información. Cabe señalar que los *servicios de seguridad* de computo varían de acuerdo a lo que se requiera o se pueda pagar, claro, por lo que no necesariamente debe de tener las características antes mencionadas, puede tener una, todas u otras distintas.		
E1_TipoC	Sí. Los *servicios de seguridad* son abstracciones de la realidad que se Utilizan para proteger la información de sus posibles *ataques.* Entre los principales *servicios de seguridad* encontramos, la *autenticación*, la *Confidencialidad*, la *integridad* y el *no repudio.*		
E2_tipoC	Sí. Servicios abstractos para dar mayor confiabilidad a los sistemas multiservicios.		
E3_TipoC			La pregunta se presta a confusiones.
E4_TipoC	Sí. Escalonamiento con que puede contar		

	una aplicación que le da un valor agregado.		
E5_TipoC			Es muy recomendable cuando la información es valiosa e importante, pero existen ocasiones en que la información no necesita protección porque es de dominio público.

5. A su criterio cuáles deberían de ser los adjetivos asociados a la información para que ésta fuese aceptada por usted para realizar su trabajo. Indique por favor su área de trabajo:

___ Administrativa ___ Diseño gráfico ___ Análisis
___ Diseño de sistemas ___ programación ___ Tomador de decisiones
___conectividad ___ otra

La información _____

Clave	Área de trabajo	Respuesta
E1_TipoA	otra	Útil.
E2_TipoA	Diseño gráfico. otra	La información debe servir para la toma de decisiones, debe servir para análisis y sobre todo, que su aplicación brinde beneficios para quien la sepa administrar.
E3_TipoA	Análisis	Precisa, disponible, oportuna, segura.
E4_TipoA	Administrativa, Tomador de decisiones.	Íntegra, real, precisa, segura.
E5_TipoA	Programación, diseño de sistemas.	No replicada, real, de disponibilidad inmediata o cuando sea necesaria, que cuente con significado, debe ser administrada, útil.
E1_TipoB	Análisis, programación, otra	Disponible, confiable, suficiente.
E2_TipoB	Tomador de decisiones	Debe ser verificable, comprobable, objetiva y oportuna.
E3_TipoB	Otra	Simplemente ser útil en el momento en el que se necesite.
E4_TipoB	Programación	Debe ser clara, concisa, estructurada, organizada y confiable
E5_TipoB	Otra	Debe ser los suficientemente clara, confiable y sencilla como para tomar una buena decisión de negocios.
E1_TipoC	Seguridad	La seguridad implica muchos aspectos, entre ellos encontramos el diseño de sistemas, la importancia de la información, el análisis de los problemas que se generan y principalmente, el viaje de la información en la red. Se sabe que las redes son canales públicos en los que cualquier persona puede tener acceso, ya sea implementando equipos Para obtener la información durante su viaje, o realizando *ataques* mediante software (hallar *vulnerabilidades* de los sistemas). Es por eso que el punto más importante de la seguridad se enfoca en las redes de telecomunicaciones, ya que ahí es el punto más vulnerable para atacar.
E2_TipoC	Seguridad	Íntegra, inmodificable sin consentimiento, administrable por personal capacitado, fluida,

		con sentido, necesaria.
E3_TipoC	Seguridad	Nuevamente, la pregunta me parece ambigua.
E4_TipoC	Seguridad, Tomador de decisiones.	Limpia, sin nada que le quite su sustancialidad, disponible, segura. Calidad de información = Costo a favor.
E5_TipoC	Seguridad	Protegida.

6. ¿Usted conoce, sabe o utiliza algún método para brindar seguridad a su información cotidiana tal como passwords, *cifrado* de información, respaldos, auditorias, etc.?			
Clave	☐ Sí, ¿cuáles?	☐ No.	☐ Otra respuesta. ¿Cuál?
E1_TipoA	Sí, logins, passwords, passphrases y encriptación de datos.		
E2_TipoA	Sí. Passwords cuando trabajo en *unix*;		
E3_TipoA	Sí. Pasworda, *firewalls*, respaldos.		
E4_TipoA	Sí. Depende del tipo de información de la cual se este hablando. Por ejemplo para brindar seguridad a nivel PC, va desde el password de arranque de la máquina, autentificación de la red, permisos y accesos a los sistemas de archivos, etc. pero si hablamos de un centro de cómputo va desde acceso restringido en sitio (físico) o por medio del software y comunicaciones (lógico). La pregunta esta muy abierta.		
E5_TipoA	Sólo passwords y biométricos.		
E1_TipoB	Sí, dispongo de un encriptador para documentos confidenciales, así como un sniffer de red y parches de seguridad del Sistema Operativo.		
E2_TipoB	Sí, password, crypt, permisos, seguridad por oscuridad, *shell* restringido, firmas criptográficas, *llaves* públicas y privadas, etc..		
E3_TipoB	Sí, passwords, encriptado, protocolos.		
E4_TipoB	Sí, pgfw: passwords se utilizan *firewallsII* y palswd+, para correo electrónico se usa PGP, para llamadas telefónicas PGP-Phone, para auditoria kerberos y para servicios TCP-Wrappers.		
E5_TipoB	Sí. Los mencionados en la pregunta.		
E1_TipoC	Sí. Existen diversos programas que se pueden utilizar, dependiendo del tipo de seguridad que se desea obtener. Para tener sesiones seguras, y transferencia de información, se puede utilizar Secure *Shell* (SSH) que es un protocolo que cifra toda la información durante su viaje en la red. Por otra parte se puede utilizar PGP para *cifrado* de mensajes. Se pueden utilizar también algoritmos de *llave* secreta como el *DES*, para intercambio de información, o algoritmos		

	de *llave* pública como RSA, para intercambio de *llaves* o firmas digitales, así como para servicios de *confidencialidad* y *autenticación*. Se pueden implementar también muchos pro-gramas de monitoreo de redes, que pueden detectar los intentos de *ataques* y el estado de los equipos conectados a la red.		
E2_tipoC	Si, herramientas de software de seguridad, políticas de uso de recursos, bitácoras y herramientas de auditoria.		
E3_TipoC	Sí. Passwords fuertes, *cifrado* de información, auditorias. No he tenido buenas experiencias con los respaldos.		
E4_tipoC	*Cifrado* de información y passwords.		
E5_TipoC	Sí, en *UNIX* existe el ssh (*shell* security) que me permite cifrar mi canal de comunicación, tanto de salida como de entrada) y PGP en el caso de envío de correo electrónico.		

7.) ¿La información sensible (indispensable) tiene alguna protección?			
Clave	☐ Sí, ¿cuál?	☐ No, ¿por qué?.	☐ Otra respuesta. ¿Cuál?
E1_TipoA	Sí. passwords, encriptación y permisos de acceso.		
E2_TipoA	Sí. Utilerías para el manejo de archivos o manipulación de los mismos, soporte de información. Sobretodo si se trata de información confidencial de los usuarios de los sistemas, que nosotros tenemos para soporte pero que por ética y políticas no debemos compartir con nadie mas.		
E3_TipoA	Sí. Passwords, control de versiones. Respaldos.		
E4_TipoA	Sí. Principalmente se cuenta con desarrollos y algunas aplicaciones administrativas que sin lugar a dudas cuentan con medidas de seguridad, inclusive se tiene un *firewall*.		
E5_TipoA		No. No sé cómo podría protegerla.	
E1_TipoB	Sí, encriptación de 64 bits.		
E2_TipoB	Sí, la información valiosa normalmente tiene por lo menos 2 respaldos en diferentes medios.		
E3_TipoB	Sí, encriptación, passwords.		
E4_TipoB			En su formato natural (origen), la información no tiene protección pues por

			naturaleza la información debe ser entendible por la entidad a quien va dirigida.
E5_TipoB			???
E1_TipoC	De entrada podemos señalar que la información sensible no posee ningún tipo de protección y es completamente vulnerable a *ataques*, para evitar esto se pueden implementar programas de acceso físico restringido, red con reglas de choque, etc.		
E2_tipoC	Sí, la administración de la seguridad de las computadoras que la almacenan, se cifra la información a través de la red interna.		
E3_TipoC	El sistema completo debe estar protegido, incluyendo toda la información que este contiene.		
E4_tipoC		No se ha considerado. Cuando llega actuamos.	
E5_TipoC	Sí, se cuenta con unidades de respaldo.		

8. ¿En el área o centro de cómputo en donde usted labora, se cuenta con algún plan que proteja las transmisiones (telecomunicaciones)?			
Clave	☐ Sí, ¿por qué?	☐ No, ¿por qué?.	☐ Otra respuesta. ¿Cuál?
E1_TipoA		No, por desconocimiento de los encargados de área.	
E2_TipoA			Del área hacia afuera si se tienen controladas las entradas desde otros equipos de cómputo, y en la red local se tienen restringidos los accesos a algunos equipos de cómputo.
E3_TipoA	Sí, Se cuenta con infraestructura propia y afecta directamente la función de la organización.		
E4_TipoA	Sí. Por que sabemos la *vulnerabilidad* de la seguridad de la información y sobre todo por una cultura de riesgos.		
E5_TipoA			No sé, necesito preguntar y que me guíen para poder proteger.
E1_TipoB	Sí, porque se checa la *integridad* de la transmisión de la información recibida o enviada.		
E2_TipoB	Sí precisamente porque debido a su importancia es indispensable tener retro-alimentación de que		

	esta llegando a su destino, o que esta haciendo lo que tiene que hacer.		
E3_TipoB	Sí, porque permite corregir errores o pedir que se manden otra vez.		
E4_TipoB		No. Como plan yo entiendo un manual de procedimientos o políticas de seguridad para la protección de transmisiones, las cuales no se encuentran documentadas, o al menos no tienen difusión entre el personal que aquí laboramos. La protección de las transmisiones es decisión y responsabilidad del usuario.	
E5_TipoB	Sí. es necesario.		
E1_TipoC	Si, se cuentan con diversos programas de *cifrado* de información, y es obligatorio el uso de ellos, por otra parte, se cuentan con programas de monitoreo de la red principal.		
E2_tipoC		No, no lo sé.	
E3_TipoC			Estamos en proceso de implementar un *firewall* y requerir conexiones encriptadas
E4_TipoC		No, no se ha planeado.	
E5_tipoC	Sí porque constantemente existe un monitoreo de los paquetes para conocer si están llegando correctamente, además de que existen utilerías que ayudan con estas tareas.		

9) ¿Y con planes de recuperación de información? Considerando respaldos, pérdidas o recuperación a intervenciones ilícitas.			
Clave	□ Sí, ¿por qué?	□ No, ¿por qué?.	□ Otra respuesta. ¿Cuál?
E1_TipoA	Sí, por seguridad y mantenimiento de a *integridad* de la información.		
E2_TipoA		No. No se tiene ni la política ni el hábito.	
E3_TipoA	Sí. Respaldos y copias de seguridad fuera de las instalaciones.		
E4_TipoA	Si. Es un plan de continuidad de operaciones (Business Continuity Planing "BCP")		

E5_TipoA		No. No sé cómo lo haría.	
E1_TipoB	Sí, se realizan respaldos a la semana o al momento que se considere necesario sobre cartuchos zip.		
E2_TipoB	Sí, cada administrador tiene a su cargo los respaldos totales e incrementales tomando en cuenta periodicidad, y debe mantener un monitoreo constante sobre los usuarios, procedencias y procesos que hay en un momento dado.		
E3_TipoB	Sí, porque la información manejada es valiosa y se requiere tener una mejor seguridad al tener respaldos.		
E4_TipoB	Sí. Se cuenta con planes de contingencia en la dependencia en que laboro, sin embargo, desde mi perspectiva, falta la difusión necesaria de las mismas Entre todo el personal. El conocimiento de los planes y su puesta en practica normalmente es responsabilidad del personal de confianza, por no llamarles Jefes.		
E5_TipoB	Sí. Los mencionados en la pregunta. Además que el uso de respaldos es una política.		
E1_TipoC	También, se tienen planes de respaldo de información, respaldo parciales (semanales) y respaldos totales (mensuales) para poder recuperar la información en caso de sufrir algún ataque.		
E2_TipoC	Sí. De toda la información que se encuentra en los sistemas se cuenta con respaldos periódicos de su información.		
E3_TipoC			Estamos esperando a que se apruebe una requisición de un equipo confiable de respaldo.
E4_TipoC	Sí. Recordemos que la información tiene un valor por lo tanto debe ser tratada como cualquier otro activo.		
E4_tipoC	Sí, se lleva un estricto control de los respaldos (semanalmente) por lo que no existe mucho problema en este aspecto.		

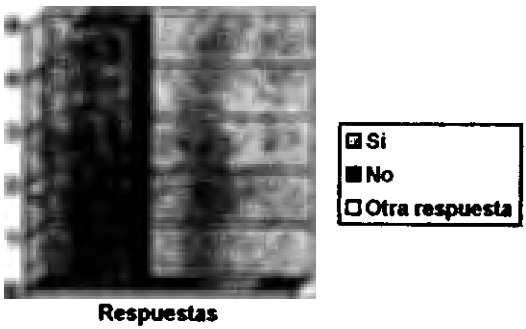
10. ¿Se realizan pruebas de detección de passwords en los sistemas de *autenticación* multiusuarios para accesos locales y remotos?			
Clave	☐ Sí. ¿por qué?	☐ No, ¿por qué?.	☐ Otra respuesta. ¿Cuál?
E1_TipoA		No porque no se han recibido *ataques* de *hackers* y nadie ha querido atacar a los servidores.	
E2_TipoA			No sé.
E3_TipoA	Sí. Se controla el acceso a los datos organizacionales debido a su interconexión con otros sistemas públicos.		
E4_TipoA			No se si se lleva a cabo.
E5_TipoA			No se cómo lo haría.
E1_TipoB		No, de ello se encarga nuestro administrador de red.	
E2_TipoB			Muy rara vez, dependiendo del equipo y su relevancia, se corren programas para detectar passwords débiles u obvios. Lo que se hace es seguir políticas como el tener que ingresar al menos dos dígitos o caracteres especiales, el tener que cambiar de password cada 30 días, etc.
E3_TipoB	Sí, el software UNISYS detecta la ubicación de los usuarios por si llega a haber alguna anomalía.		
E4_TipoB		No.	
E5_TipoB		No.	
E1_TipoC	Si, de hecho el acceso remoto a la red esta muy controlada, y solo se pueden obtener accesos remotos previa solicitud y motivos, estas cuentas se monitorean constantemente. Por otra parte existen políticas de cambios de passwords, mediante el sistema utilizado es posible informar a los usuarios que deben cambiar sus passwords cada cierto tiempo (tres meses, por ejemplo)		
E2_tipoC	Sí, como SSH (secure *shell*), password++, S-Key.		

E3_TipoC	Sí. Las cuentas con cierto privilegio deben ser constantemente monitoreadas y revisadas.		
E4_TipoC	Sí. Se utiliza Tripwire y COPS.		
E5_tipoC	Sí, por el momento sólo se utiliza la última versión de CRACK (CRACK 5), el cual es manejado a través de un diccionario enorme, lo que me permite que mis usuarios tengan passwords seguros (y ver cuáles son inseguros claro).		

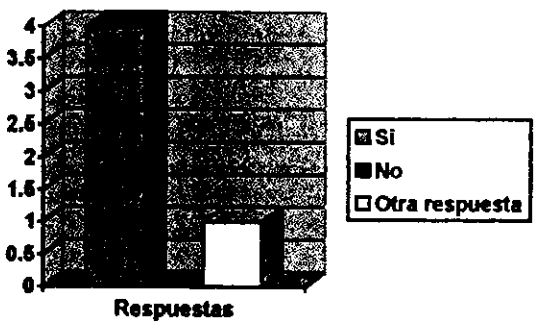
Anexo I-5

Conclusiones derivadas de la aplicación de los cuestionarios y las entrevistas a las personas referidas en "conocimiento empírico en el medio" y en "opiniones profesionales"

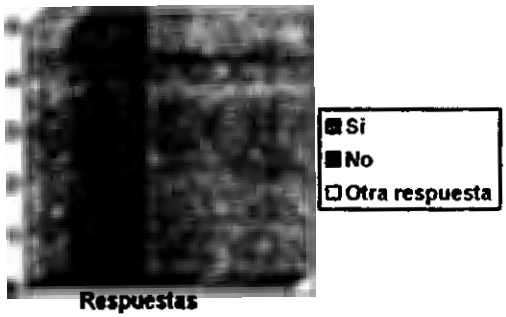
Respuestas de las personas tipo A para la pregunta No. 1.



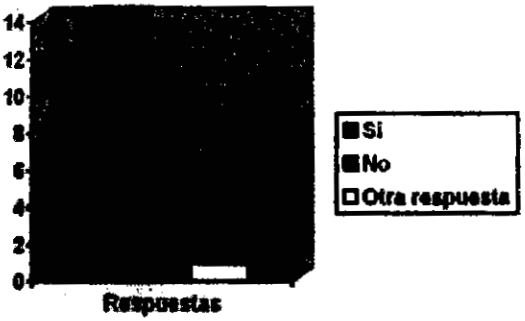
Respuestas de las personas tipo B para la pregunta No. 1



Respuestas de las personas tipo C para la pregunta No. 1



Respuestas de todas las personas a la pregunta No. 1.



Conclusión: Si se dio la respuesta esperada.
De las 15 personas a las que se aplicó el cuestionario, 14 de ellas creen conveniente el que se estudien los riesgos y las *vulnerabilidades* que afectan a la información que existe en un centro de cómputo.
Las respuestas independientemente de las diferencias en los grupos fueron parecidas.

Respuestas de todas las personas para la pregunta No. 2.
Únicamente se toman las ideas fundamentales y se evita colocar duplicidad de datos. En otros casos se sustituyen algunos términos expresados por las personas entrevistadas por términos que se han manejado hasta este momento en este trabajo.

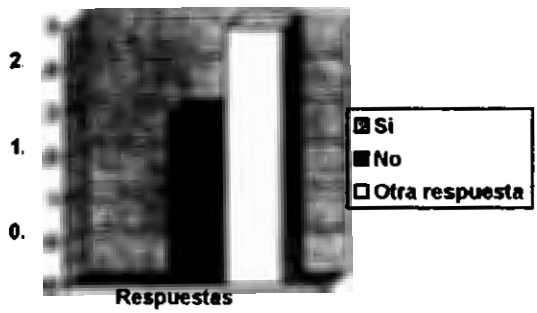
Personas tipo A		Personas tipo B		Personas tipo C	
Beneficios o ventajas	Desventajas	Beneficios o ventajas	Desventajas	Beneficios o ventajas	Desventajas
Evitar pérdida de información Serviría para integrar *servicios de seguridad* Robustecer los	Es caro. Hacer públicos los resultados del *análisis de riesgos* invitaría a personas a	Estimación de costos de mantenimiento. Mejor control de riesgos. Creación de planes	Tiempo Costo	Descubre y disminuye las vulnerabilidades en los equipos, accesos y	Es imposible eliminar un riesgo por completo, en ese sentido todo gasto es

sistemas Planeación de contingencias y procedimientos alternos. Mitigar riesgos.	dañar a la organización. Puede derivar que el área de sistemas salga muy mal en la evaluación.	de contingencia. Protección de los datos. Continuidad en la operabilidad. Concientización. Protección a los activos fijos.		sistemas. Permite llevar una administración de las herramientas a usar. Protección de los activos. Optimiza costos. Mayor confiabilidad en la información	infructuoso. El hacer un *análisis de riesgos* correcto requiere mucho tiempo de elaboración. Costo.

Quizá las respuestas más interesantes son las dadas por los entrevistados de la clase C, en primer lugar son los únicos que mencionaron como ventaja el encontrar las *vulnerabilidades* a las que se podría enfrentar el organismo.

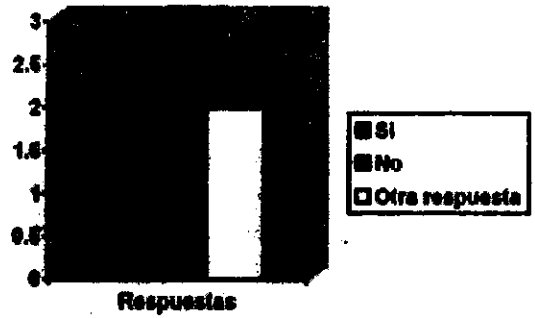
Un dato curioso, para los entrevistados del tipo A y tipo B consideran como desventaja el costo derivado del análisis de riegos, sin embargo para algunos entrevistados tipo C consideran que el realizar un *análisis de riesgos* ayudará a disminuir su costo de operación pero otros opinaron que puede resultar caro.

Respuestas de las personas tipo A para la pregunta No. 3.

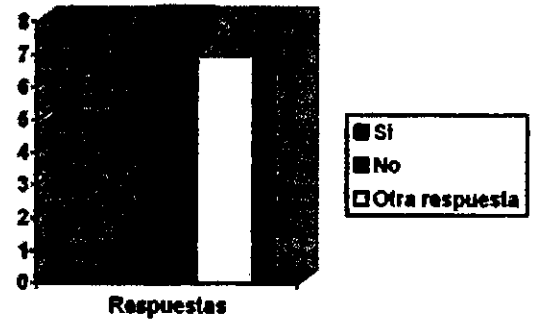


Respuestas de las personas tipo B para la pregunta No. 3.

Respuestas de las personas tipo C para la pregunta No. 3



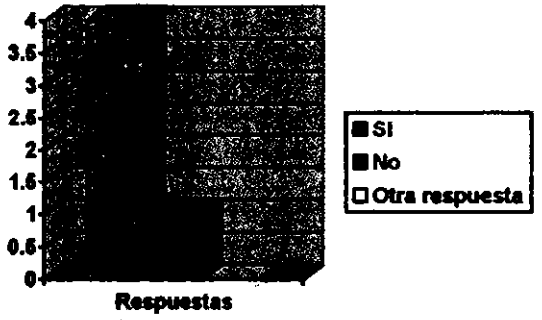
Respuestas de todas las personas para la pregunta No. 3



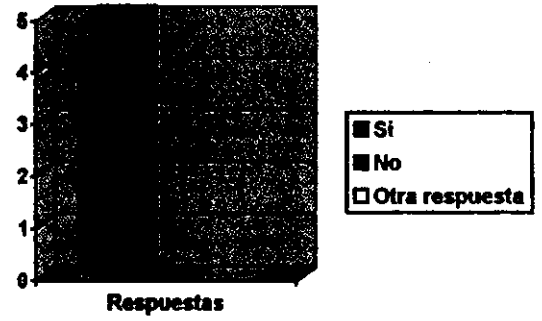
Conclusión: No se dio la respuesta esperada.

De las 15 personas entrevistadas ninguna respondió afirmativamente, lo que quiere decir que independientemente del grado en conocimiento de seguridad todas las personas saben que la información que obtienen de un sistema no es segura.

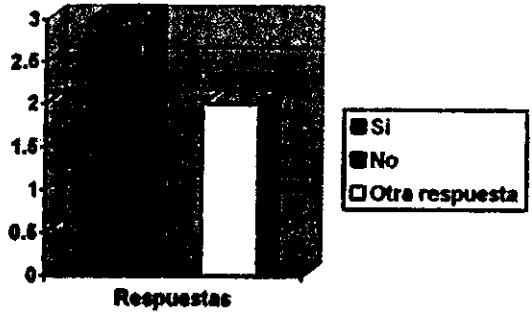
Respuestas de las personas tipo A para la pregunta No. 4.



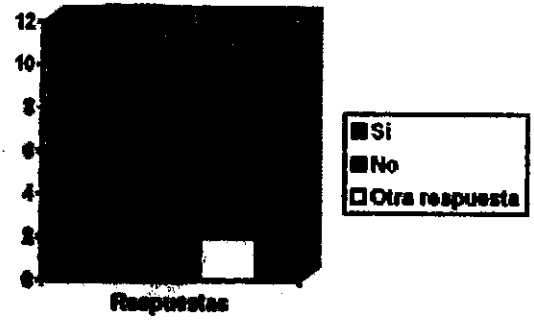
Respuestas de las personas tipo B para la pregunta No. 4



Respuestas de las personas tipo C para la pregunta No. 4



Respuestas de todas las personas para la pregunta No. 4.



Conclusión: No se dio la respuesta esperada.
A pesar de que la respuesta en su casi totalidad fue si, muchas de las respuestas son erróneas. En otros casos afirman y describen a un *servicio de seguridad* pero entre su definición hay cosas ciertas y hay otras que no lo son. De tal manera que a pesar de señalar una respuesta afirmativa de manera personal se optaría por declarar la respuesta como "Otra respuesta".
Lo que influyó en este tipo de contestaciones es que muchos de los entrevistados desconocen el concepto de "*servicio de seguridad*" en materia de seguridad, de echo solo 3 personas del tipo C contestaron de manera precisa, las personas del tipo A y B tomaron el significado común de las dos palabras "servicio" y "seguridad" y estructuraron sus respuestas.

Respuestas de las personas tipo A para la pregunta No. 5.
Nuevamente, no se duplican datos y en su momento se reemplazan algunos conceptos.

- Útil, debe servir para la toma de decisiones, precisa, disponible, segura, no replicada, real.

Respuestas de las personas tipo B para la pregunta No. 5.

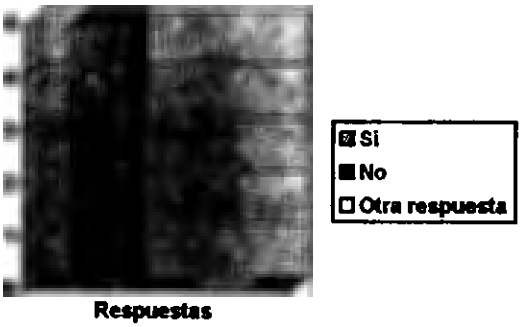
- Disponible, confiable, suficiente, verificable, comprobable, objetiva, oportuna, clara, estructurada, que sirva para tomar decisiones de negocios.

Respuestas de las personas tipo C para la pregunta No. 6.

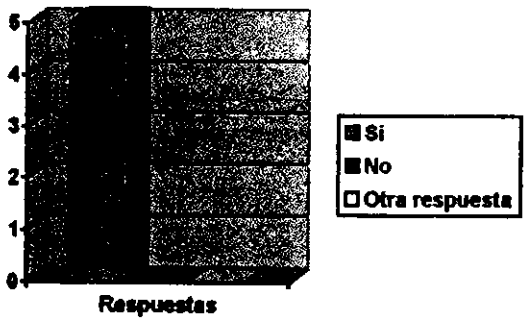
- Íntegra, inmodificable sin consentimiento, administrada, fluida, correcta, protegida.

Conclusión: Si se dio la respuesta esperada aunque no se hizo mención como se esperaba de los *servicios de seguridad* asociados a la información que se esperaría se trabajase con ella.
En esta pregunta las personas tipo A y B tuvieron muchísimas semejanzas en sus respuestas. Ambos tipos de personas mencionaron que la información debe servir para tomar decisiones. Quizá las personas del tipo C nombraban un concepto general como "administrada" en el que se referían a varias actividades contenidas que los otros grupos si hacen mención de manera explícita.

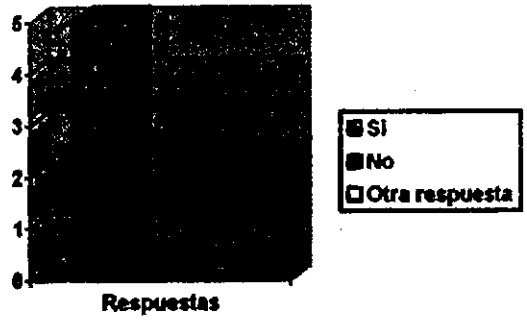
Respuestas de las personas tipo A para la pregunta No. 6.



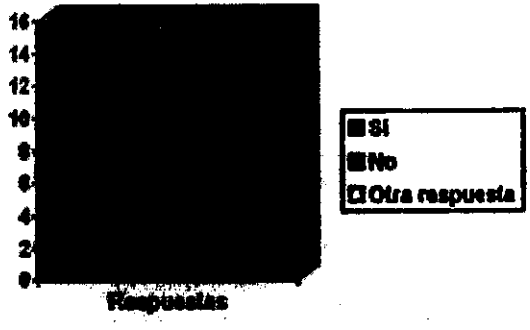
Respuestas de las personas tipo B para la pregunta No. 6.



Respuestas de las personas tipo C para la pregunta No. 6.

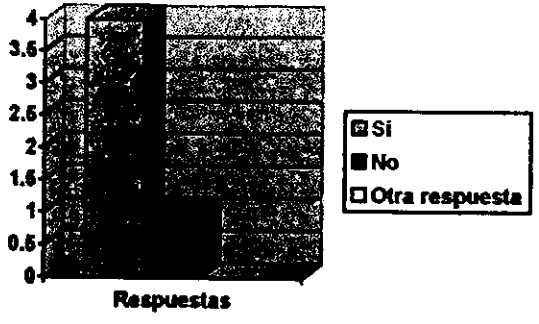


Respuestas de todas las personas para la pregunta No. 6.

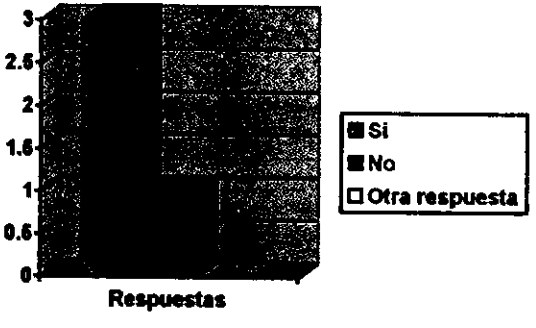


Conclusión: Si se dio la respuesta esperada.
Todos los usuarios utilizan passwords para ciertas aplicaciones. Los respaldos es lo siguiente en frecuencia de contestaciones. Las personas del grupo C utilizan herramientas especiales de seguridad y están más familiarizados con términos de cifrado de información.

Respuestas de las personas tipo A para la pregunta No. 7.

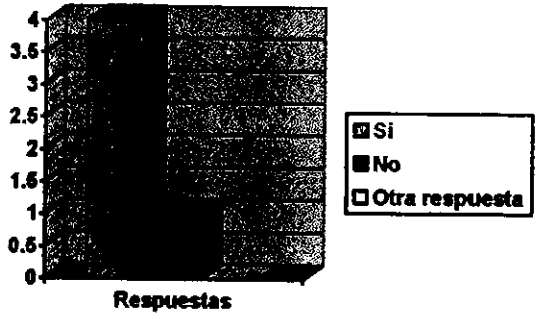


Respuestas de las personas tipo B para la pregunta No. 7.

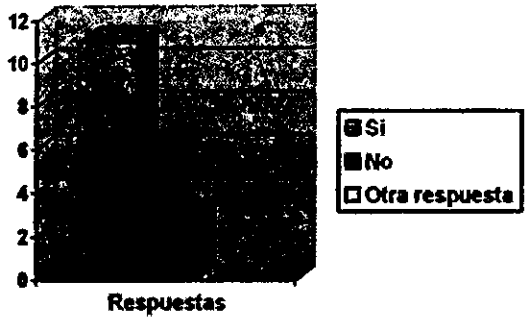


Una persona no supo qué contestar.

Respuestas de las personas tipo C para la pregunta No.7.

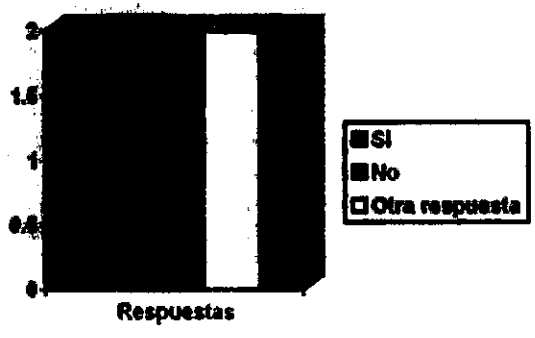


Respuestas de todas las personas para la pregunta No. 7

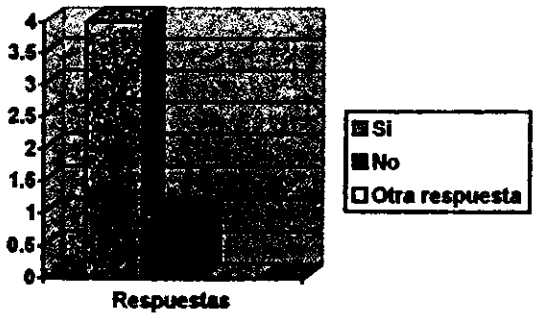


Conclusión: No se dio la respuesta esperada.
Se esperaba que la respuesta fuera no, no se cuenta con alguna protección la información sensible. Sin embargo 11 de las 15 personas argumentan que si protegen la información sensible, sin embargo en varias de las respuestas de las personas tipo A y tipo B mencionan que la protección que utilizan para la información sensible es vía password, cosa que en la práctica es poco confiable.
Hubo una abstención de responder por parte del bloque tipo B.
Un dato curioso es que una de las personas de tipo C respondió que no se había considerado implementar una protección a la información sensible, pero cuando llegue su momento probablemente si.

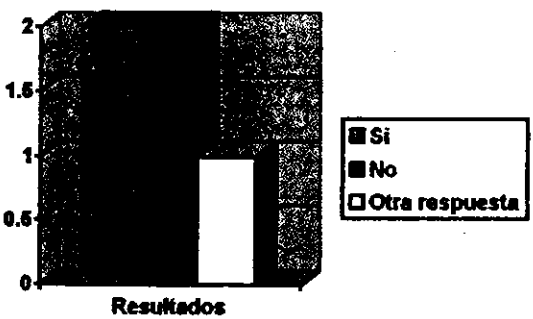
Respuestas de las personas tipo A para la pregunta No. 2.



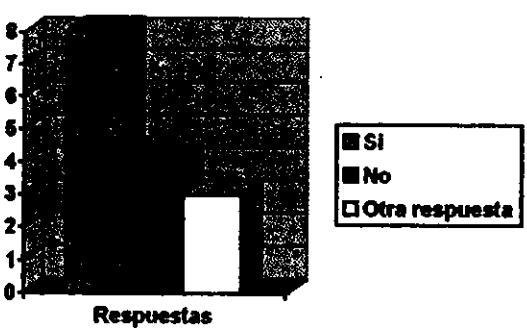
Respuestas de las personas tipo B para la pregunta No. 8.



Respuestas de las personas tipo C para la pregunta No. 8.

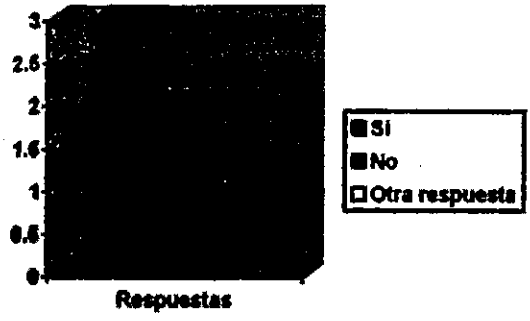


Respuestas de todas las personas para la pregunta No. 8.

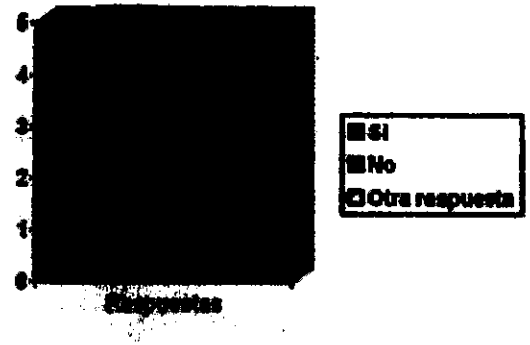


Conclusión: Sí se dio la respuesta esperada.
Todas las contestaciones derivan que por lo menos se tiene conocimiento teórico de los peligros que corre la información durante la transmisión hacia un equipo.

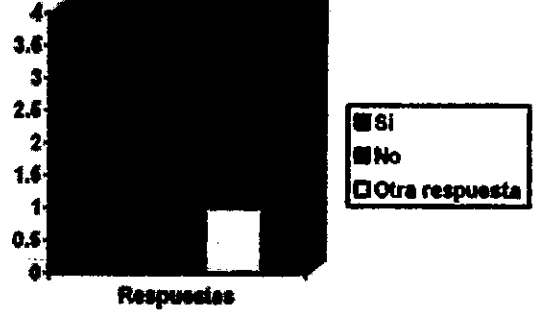
Respuestas de las personas tipo B para la pregunta No. 9.



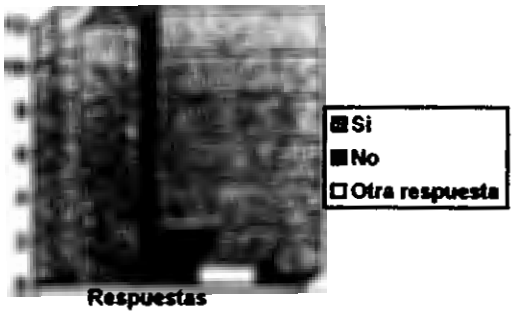
Respuestas de las personas tipo B para la pregunta No. 9.



Respuestas de las personas tipo C para la pregunta No. 9.

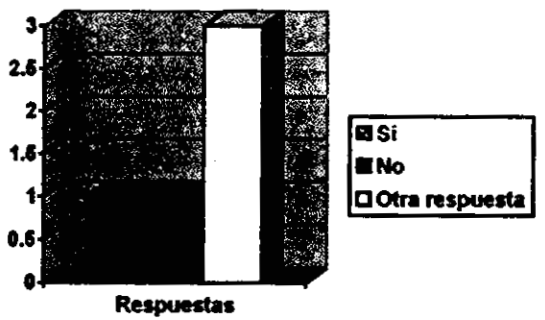


Respuestas de todas las personas para la pregunta No. 9.

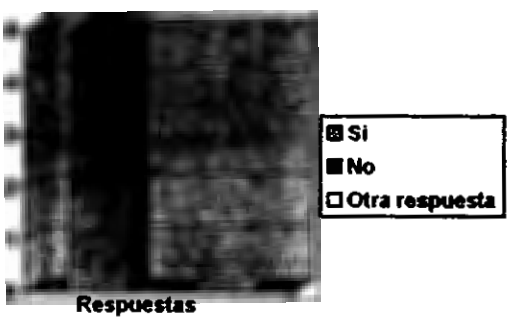


Conclusión: Si se dio la respuesta esperada.

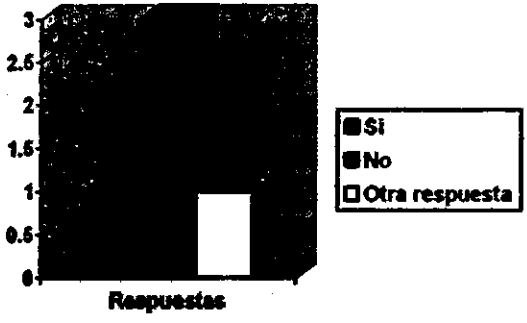
Respuestas de las personas tipo A para la pregunta No. 10.



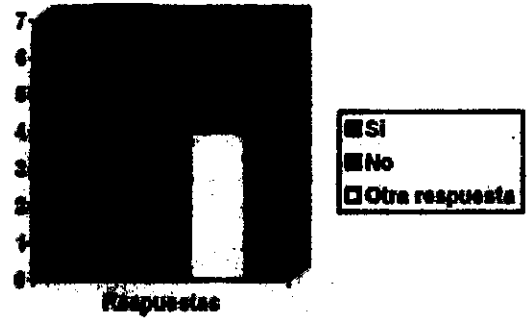
Respuestas de las personas tipo B para la pregunta No. 10.



Respuestas de las personas tipo C para la pregunta No. 10.



Respuestas de todas las personas para la pregunta No. 10.



Conclusión: Si se dio la respuesta esperada aunque cabe señalar lo siguiente:
Para cada grupo de personas entrevistadas se tuvieron distintas frecuencias en las respuestas. La respuesta que tuvo la mayoría fue "no sé". Para el caso de las personas de tipo B la respuesta fue "No". Sin embargo para el 100 % de las personas de tipo C la respuesta fue "Si".

1.10 Referencia bibliográfica.

El Hilo de la Modernidad
Notas sobre la informática en México y el caso de la UNAM.
Felipe Bracho. Investigador del Instituto de Investigaciones en Matemáticas Aplicadas y en sistemas (IIMAS) de la UNAM.

Microsoft Press
Computer Dictionary
(usado para tomar el concepto de "sistema abierto").

Reglamento general de exámenes.
1997
Universidad Nacional Autónoma de México.

RV Cómputo.
Celebración de los 40 años de Cómputo en México.

II. MARCO TEÓRICO.

2.1. Introducción.

En esta fase se consideran dos cosas fundamentales:

El conocimiento de las fuentes de información.
El registro de los datos:
De las fuentes (datos del libro).
De la información (descripción del material útil).

Para recabar información se necesita saber en dónde puede encontrarse, por lo tanto es recomendable establecer algunos sitios de referencia. Para estudios como éste lo recomendable es mantener una referencia actualizada basada en bibliografía especializada y enlaces de internet.

2.1.1. - El conocimiento de las fuentes de información.

Las fuentes de información son muy variadas, se pueden clasificar de la siguiente manera:

Fuentes de Información.	Documental	Bibliográfica (libros obtenidos ya sea por librerías y/o por bibliotecas). Tesis (Por su naturaleza caen dentro de la clasificación bibliográfica pero merecen una mención especial). Hemeroteca[12]. a) Revistas. b) Periódicos. Seminarios (conferencias). Congresos. Mesas redondas (paneles, foros). Videoteca o cineteca (películas). Internet. Investigación actualmente desarrollada. La Dra. Guillermina Baena aporta además los siguientes tópicos: Archivos históricos y/o administrativos (banco de datos). Audioteca o Fonoteca. Iconoteca o museo. Centro de información o centro de Informática.
	De campo	XIV. Observación. XV. Interrogación. Entrevista. Encuesta.

Del cuadro anterior podemos establecer dos definiciones útiles para este estudio: Información documental; e

[12] Del griego *hemera* "día" y *theke* "caja, depósito".

Información de campo.

Documental según su sentido etimológico significa:
Gr. *docére*: enseñar.
Gr. *mentum*: instrumento, medio.
Lat. *alis*: relación, conformidad, semejanza.

Se puede definir "información documental" como aquella información obtenida por medio de documentos, es decir con los instrumentos escritos existentes, utilizados para obtener un conocimiento.

Campo etimológicamente significa:
Lat: campus: terreno.

Se puede definir "información de campo" como aquella información que no se encuentra escrita y que para obtenerla habrá que trasladarse a algún lugar específico para obtenerla.

2.1.2. El registro de los datos.

a) De las fuentes.

Para cada fuente utilizada corresponderá su referencia trátese de libro, revista, biblioteca, dirección internet, persona, etc.

b) De los datos.

Dependiendo del tipo de material utilizado se hará mención de la información obtenida en o de él.

2.2. Libros.

A)Libros de estudio

Son libros cuyo contenido general o bien la mayoría del libro servirá para retomar en el trabajo de tesis.

a)
Nombre: "Determinación de riesgos en los centros de cómputo"
Autor: Humberto David Rosales Herrera.
Editorial: Trillas.
Primera edición septiembre de 1996.

ISBN: 968-24-5461-1

Explicación sintética de cada capítulo.

Libro integrado por tres capítulos y dos apéndices. La dinámica de la lectura desarrolla una metodología para determinar los distintos riesgos a los que se encuentra un centro de procesamiento de información en escenarios de hace poco más de 4 años.

Capítulo 1. "Exposición analítica". Presenta el desarrollo de los ambientes en los que los sistemas de información computarizados se encuentran sujetos a eventualidades capaces de romper su dinámica e indica la manera en la que se pueden generar errores que pudieran ocasionar desequilibrios organizacionales.
El autor clasifica estos hechos imponderables según su naturaleza en involuntarios, imprudenciales intencionados y naturales. La probabilidad de ocurrencia de esos eventos es denominada riesgo. Los sistemas de información computarizados son diseñados para satisfacer las necesidades de procesamiento de datos, donde es contemplado en mayor grado una serie de controles que permitan reducir el impacto que podrían ocasionar los problemas generados por cualquier hecho eventual. Se hace hincapié en que en la práctica existen circunstancias que dentro del procesamiento electrónico de datos impiden mantener un nivel óptimo en el funcionamiento de los sistemas y, por ende, el de los centros de cómputo.
El resto del capítulo es un desarrollo de ideas según las cuales el autor trata de identificar la existencia de *vulnerabilidades* en los sistemas de información. Pretende presentar un análisis sobre los principales riesgos que implica un ambiente de procesamiento de datos y cómo tratar de descubrirlos para determinar su relevancia y establecer las prioridades requeridas a fin de elaborar un plan de acción que permita solucionar de manera eficiente el problema detectado.

Capítulo 2. "Contexto crítico". Parte de la siguiente premisa: La creciente aplicación de las computadoras para resolver los problemas del control de la información en una forma más eficiente ha hecho de los centros de cómputo unos sitios de moda con controles mínimos necesarios para operar bajo un ambiente de seguridad, confiabilidad y *confidencialidad*, y es un punto muy vulnerable para las empresas.
Este capítulo abarca varios de los controles que pueden aplicarse para tener un escenario de seguridad "más agradable", pasando por la descripción de controles de pre-instalación, controles de organización, controles de desarrollo, controles de operación, controles de procesamiento y controles de documentación.
Se da un énfasis especial a la auditoria informática como una manera de determinar los puntos vulnerables de la seguridad informática. Da una referencia concisa sobre el cómo desarrollar una planeación del proyecto de auditoria.

- Capítulo 3. "Integración". En este capítulo se concluye que la existencia de los riesgos dentro del procesamiento electrónico de datos se debe básicamente a tres factores fundamentales:

1.- Falta de capacitación sobre los aspectos que se deben cubrir para el óptimo uso de los recursos computacionales.
2.- Falta de integración del área de procesamiento electrónico de datos con respecto al resto de los departamentos de la organización.
3.- Falta de una planeación estratégica dentro de la organización en relación con el procesamiento electrónico de datos.

Apéndice A.- Contiene una matriz que relaciona riesgos, controles y procedimientos de revisión.

Apéndice B.- Contiene un análisis del efecto del procesamiento electrónico de datos y su relación con un procesamiento de auditoria.

b)
Nombre: "Computer Crime. A Crimefighter's Handbook"
Autores: David Icove, Karl Seger & William VonStorch.
Editorial: O'Reilly & Associates, Inc.
Primera edición agosto de 1995.
ISBN: 1-56592-086-4

Explicación sintética de cada capítulo.

Este libro trata de manera general una introducción a los conceptos de delitos en computadoras. Esta dirigido hacia personas que comienzan a interesarse en tales conceptos de criminología particular. Entre esas personas se encuentran todas aquellas que laboran en organizaciones que utilizan computadoras, administradores, legistas, personal de *seguridad física* y personal de seguridad lógica. Se incluyen temas interesantes para personas que se hayan enfrentado en su organización con algún delito computacional y que necesite conocer cómo proceder después de éste. Los delitos que abarca particularmente son delitos de equipos conectados a internet o a una red local.

El libro esta dividido en 5 partes, 4 apéndices y un glosario.

Parte I. "Overview". Introduce al tema de delitos computacionales, bosqueja los mayores tipos de delitos en cómputo y tipos de delincuentes que podrían manifestarse y da una descripción de las principales leyes de los Estados Unidos que son utilizadas para proseguir contra delitos de esta naturaleza.
Esta primer parte contiene 4 capítulos.
Capítulo 1. "Introduction to computer Crime". Describe un número de diferentes tipos de *ataques* en centros de cómputo gubernamentales y de la iniciativa privada (norteamericanos) y proporciona un panorama de algunos riesgos en sistemas de cómputo.

Capítulo 2. "What are the crimes?". Describe las categorías de incidentes en cómputo que el autor clasifica en cuatro rubros:
Incidentes de *seguridad física*.
Incidentes de seguridad del personal.
Incidentes de las comunicaciones y seguridad de los datos.
Incidentes de la seguridad de las operaciones.
El capítulo concluye con algunas recomendaciones para detectar *ataques* comunes.

Capítulo 3. "Who commits computer crimes?". Detalla las diferentes categorías de delincuentes e materia de cómputo.

Capítulo 4. "What are the laws?". Presenta un resúmen de las principales leyes que prohiben los delitos computacionales.

Parte II. "Preventing computer crime". Esta parte aborda las maneras detectadas por el autor para prevenir delitos en materia de cómputo. Identifica los riesgos que afectan a los sistemas computacionales y declara algunas medidas de seguridad que pudieran proteger a los sistemas.

Capítulo 5. "What is a risk?". Identifica los activos de un centro de cómputo y sistemas de información y bosqueja amenazas, *vulnerabilidades* y medidas de seguridad en cómputo.

Capítulo 6. "Physical security". Describe las amenazas a la *seguridad física* (natural y desastres ambientales) y presenta medidas para mitigar esos riesgos.

Capítulo 7. "Personnel security". Discute brevemente los componentes importantes de un programa de seguridad del personal para varios tipos de personas, incluyendo empleados, vendedores, clientes y otros.

Capítulo 8. "Communications security". Describe las amenazas a los sistemas que se encuentran en red y las técnicas para mitigar esas amenazas (passwords, *cifrado* de las transmisiones, *firewalls*, etc).

Capítulo 9. "Operations security". Describe cómo la seguridad de las operaciones se relaciona con otros tipos de medidas de seguridad. Las operaciones de seguridad incluyen maneras de incrementar la conciencia de las ocurrencias de posibles delitos en cómputo. Actualmente la manera de prevenir tales delitos en cómputo es encontrar la manera en cómo éstos ocurren.

Parte III. "Handling computer crime". Esta parte describe la manera en como hay que planear la detección e investigación ante un delito computacional".

Capítulo 10. "Planning how to handle a computer crime". Discute las varias maneras en cómo se pueden detectar delitos computacionales, además indica la manera en como se

puede crear un equipo de administración de crisis y las consecuencias a considerar antes de que ocurra un delito informático.

Capítulo 11. "Investigating a computer crime". Esboza un procedimiento para investigar y darle seguimiento a un delito computacional, describe el papel de un "equipo de investigación", discute la preparación de una búsqueda de pistas y describe la manera de colectar y proteger las evidencias.

Capítulo 12. "Prosecuting a computer crime". Discute los problemas especiales involucrados al describir los delitos en cómputo en un tribunal de justicia, la publicación de pruebas tales como los problemas de rumores, sugerencias en las testificaciones sobre los delitos en cómputo donde hay muchos conceptos no retomados aun por las leyes y que se utilizan para testificar.

Parte IV. "Computer crime laws". Contiene una lista completa de textos de las principales leyes norteamericanas que se prohiben los delitos en materia de computo. Van desde leyes de algún estado norteamericano hasta algunas referencias de leyes internacionales hasta el momento en el que el libro fue publicado.

Parte V. "Apéndices". Contiene un resumen de recursos y artículos que explican algunos conceptos utilizados a lo largo del libro.

Apéndice A. "Resources summary". Contiene una lista de recursos que podrían ser de mucha ayuda para prevenir, investigar y darle seguimiento a los delitos en cómputo. Incluye referencias de libros, periódicos y recursos en línea relevantes en materia de delitos en cómputo.

Apéndice B. "Raiding the computer room". Artículo realizado por John Sauls acerca de la dimensión de las evidencias de los delitos en cómputo de hoy en día.

Apéndice C. "The microcomputer as evidence". Artículo de Michael G. Noblett acerca de la examinación de evidencias de delitos en cómputo.

Apéndice D. "A sample search warranty". Es un citatorio ante un juez derivado de una investigación de un delito en cómputo cometido en una universidad.

Glosario. Define los términos técnicos utilizados en este libro.

c)
Nombre: "Seguridad de la información en sistemas de cómputo".
Autor: Luis Angel Rodriguez.
Editorial: Ventura
Edición junio de 1995.

ISBN: 968-7393-20-3
Url: http://www.alfaomega.com.mx

Explicación sintética de cada capítulo:
Libro integrado por 10 capítulos y 2 apéndices.
Capítulo 1. "Generalidades". Se presentan aspectos generales de los temas que a lo largo del libro se desarrollan con mayor o menor profundidad, entre ellos, seguridad de la información, planes de contingencia, la relación entre estos dos, su importancia, etc.

Capítulo 2. "La seguridad de la información". Se interna un poco más en el tema que constituye el conjunto en el que se encuentran los planes de contingencia. Se describen las principales amenazas a todos los componentes del procesamiento de información, clasificadas y agrupadas en grandes rubros. Se incluyen algunas ideas referentes a los seguros contra pérdida o daños de información y de equipos.

Capítulo 3. "*Seguridad física*". Se describen los riesgos que afectan la seguridad de las instalaciones físicas de cómputo. Estos riesgos pueden ser externos o internos a la empresa. Las medidas de *seguridad física* deben tomar en cuenta riesgos como accidentes, desastres naturales, *ataques* por *intrusos*, condiciones medioambientales, etc. Se describen medidas de prevención y mitigación contra estos riesgos.

Capítulo 4. "Seguridad lógica". Están incluidos los riesgos que afectan la seguridad de la información en sí. Estos riesgos también pueden ser internos o externos a la empresa. Se describen las medidas de prevención y mitigación contra estos riesgos.

Capítulo 5. "Seguridad en redes y comunicaciones". Capítulo en el que hace énfasis las redes de computadoras y las comunicaciones. Se describen los riesgos que afectan a la información cuando se transmite de una computadora a otra para posteriormente definir las medidas para prevenir y mitigar dichos riesgos.

Capítulo 6. "De los *virus* y otros demonios". Información acerca de los *virus*, la amenaza que representan, cómo descubrir su presencia y como prevenir el contagio, o en caso de ser contagiado, mitigar sus efectos.

Capítulo 7. "*Análisis de riesgos*". Presenta un panorama general. Dado que este libro es práctico se presenta este capítulo de forma muy simplificada y abreviada. La metodología que se presenta se puede utilizar de manera muy rápida y sin mayor problema.

Capítulo 8. "Plan de contingencias". Presenta el marco conceptual de los planes de contingencia. Se incluyen conceptos que un diseñador de planes debe conocer antes de iniciar el desarrollo del mismo. Se incluyen dos metodologías para desarrollo de planes de contingencia: la de Hewlett-Packard y la de William Toigo.

Capítulo 9. "Metodología propuesta". Se describe la metodología de desarrollo de planes de contingencia que el autor propone en este libro. Según palabras del autor esta

metodología es apropiada para empresas de mediano tamaño radicadas en la zona metropolitana de la *Ciudad de México* y debe aplicarse de manera muy sencilla en empresas con una dependencia importante en sus sistemas de información como las financieras. Al final del capítulo se incluye una sencilla evaluación de la metodología y se emiten algunas conclusiones.

Capítulo 10. "Auditoria informática". Este capítulo no sirve para desarrollar una auditoria sino más bien proporciona una idea de la utilidad e importancia de la auditoria informática. Se decidió incluir este capítulo porque se consideró que una buena aplicación de la auditoria informática coadyuva mucho a alcanzar los objetivos de la seguridad de la información.

Apéndice 1. Contiene las definiciones de los desastres de probable ocurrencia en México.

Apéndice 2. Contiene una serie de directorios de proveedores de productos y servicios para implementar programas de seguridad de la información y planes de contingencia.[13]

d)
Nombre: "Seguridad en centros de cómputo. Políticas y procedimientos".
Título de la obra en inglés: "A handbook for management"
Autor: Leonard H. Pine.
Editorial: Trillas.
Primera edición abril de 1988.
ISBN: 968-24-2678-2
Clasificación de la biblioteca Central de la UNAM: QA76 .9A25 F5518.

Explicación sintética de cada capítulo:
Libro integrado por 12 capítulos y 6 apéndices.

Capítulo 1. "Un enfoque nuevo sobre la seguridad en computación: concepto de seguridad total". Capítulo donde el autor se nota preocupado por la complejidad creciente y del alcance del uso de la computación que ha propiciado que la información se concentre en manos de unas cuantas personas. Según el autor, el punto de vista tradicional otorga mayor atención a los aspectos de seguridad "visibles", como el acceso físico, la extinción de incendios y la seguridad de los archivos restándole importancia a los aspectos "no visibles". La seguridad efectiva en computación requiere la revaloración de un amplio número de aspectos descritos dentro del concepto de "seguridad total" donde se encuentran ambos aspectos.

[13] Estas referencias son de empresas norteamericanas.

Capítulo 2. "Definición de una política de seguridad en computación". Trata los aspectos que se deben considerar en la definición de una política de seguridad y los elementos del método para realizar esta labor.
No existe un sistema completamente seguro y, en última instancia se depende en gran medida de la *integridad* de las personas en una empresa. La aplicación significativa de la seguridad para las computadoras requiere:
Clasificar cada instalación en términos de riesgo alto, medio o bajo.
Identificar las aplicaciones de alto riesgo, y de entre estas los programas y los archivos, que constituyen alto riesgo.
Cuantificar el riesgo, de preferencia en términos financieros.
Evaluar estrategias opcionales de seguridad y seleccionar la que resulte más apropiada para la institución.
Justificar ante la gerencia el costo de la estrategia seleccionada.
Un enfoque orientado a lograr un compromiso firme.
El compromiso de la gerencia con la política de seguridad es primordial. Éste se logra mejor por medio de la participación de todos los interesados en el trabajo previo para definir la política de seguridad.

Capítulo 3. "Organización y división de responsabilidades". La forma en como se organizan las actividades de cómputo incluye cuatro aspectos que afectan la seguridad en computación:
División de responsabilidades.
Sistemas de control interno.
Asignación de responsabilidad en cuanto a la seguridad.
Sustitución del personal clave.

Capítulo 4. "*Seguridad física* y contra incendios". Trata: ubicación y construcción del centro de cómputo. Aire acondicionado. Suministro de energía. Riesgo de inundación. Acceso. Protección, detección y extinción de incendios. Mantenimiento.

Capítulo 5. "Políticas hacia el personal". Elemento importante dentro de la seguridad en computación. Sin embargo, la dependencia exagerada en ellas es común, sobre todo en las instalaciones de alta seguridad. Se deben considerar ciertos factores como parte de las políticas hacia el personal, principalmente la contratación, los procedimientos para evaluar el desempeño, los permisos, la rotación de los impuestos y las actitudes generales. Muchos de estos aspectos se verifican de manera rutinaria fuera de la función del procesamiento de datos, pero de forma irregular dentro de ésta.

Capítulo 6. "Los seguros". No aplica para el caso de este trabajo de tesis.

Capítulo 7. "Seguridad de los sistemas". Según el autor, la seguridad de los sistemas se refiere de manera principal a la seguridad del equipo de cómputo, e incluye:
El equipo.
Los programas de uso general, es decir, se excluyen los programas de aplicación específica.

Las redes, o sea, las líneas y sistemas de comunicación de datos.
Las terminales y los programas generales directamente asociados.

Capítulo 8. "Seguridad de las aplicaciones". Abarca tanto a los componentes de la computadora como a los que no lo son, en cada aplicación. Por otra parte de la computadora comprende datos, programas y archivos que se procesan en el sistema. Los elementos que no son de la computadora incluyen recolección y entrega de datos e información del archivo maestro para el procesamiento, así como el control de dicha información para garantizar que se procese en forma correcta y su distribución lleve al usuario. Las etapas clásicas de cada sistema implican:
Iniciación manual del origen de los datos.
Conversión de los datos a un formato aceptable por la computadora, es decir, captura de datos.
Procesamiento.
Distribución de los resultados.

Capítulo 9. "Estándares de programación y operación de sistemas". Los estándares de sistemas, programación y operación, así como la documentación, tiene efectos de suma importancia en la seguridad en computación. Los requisitos de seguridad se deben revisar en forma periódica como parte del proceso de planeación computacional a largo plazo, así también como el desarrollo y la realización de las aplicaciones individuales.
La existencia de métodos de trabajo efectivos mejora la seguridad y ofrece la documentación adecuada como un derivado. Se debe considerar de manera cuidadosa el acceso a esta documentación, a fin de reforzar la división de las responsabilidades. Las copias auxiliares de toda la documentación se deben almacenar en algún lugar distante.

Capítulo 10. "Función de los auditores tanto internos como externos". Parte del concepto de seguridad total. El propósito de este capítulo es demostrar que la función de auditoria también es un elemento muy importante que se debe considerar. A pesar de que no se presenta una exposición en detalle de las técnicas de auditoria informática el impacto que tiene sobre la seguridad en computación es realmente fuerte.

Capítulo 11. "Planes y simulacros para la recuperación en caso de desastres". La prueba real de la efectividad de la seguridad es la respuesta que se produzca en el caso de un desastre real. La respuesta efectiva sólo puede proceder de los planes efectivos contra desastres, así como también del personal bien adiestrado en lo que hay que hacer según el tipo específico de desastre. Por lo tanto, la buena planeación contra desastres debe abarcar:
Las aplicaciones en proceso de desarrollo.
Las aplicaciones terminadas.
Los procedimientos para los distintos tipos de desastres.
La existencia de los planes contra desastres se debe probar por medio de los simulacros sorpresa de desastres. Estas pruebas de desastres se deben usar para reforzar y mejorar los planes contra desastres.

Capítulo 12. "Aplicación de la seguridad efectiva en computación". La seguridad efectiva en computación se logra mejor mediante el establecimiento de un comité de seguridad computacional. El comité debe asumir la responsabilidad de coordinar la revisión de la seguridad en computación de manera regular y sorpresiva, así también como de realizar la acción apropiada. El hecho de que el comité de seguridad se reúna de manera regular garantiza el seguimiento regular de las actividades, así como también que la prioridad de la seguridad en computación no se desprecie con el transcurso del tiempo.

Apéndice 1. Inventario de riesgos de seguridad en computación.

Apéndice 2. Revisión de la seguridad en computación.

Apéndice 3. Revisión de la seguridad en computación.

Apéndice 4. Un caso de estudio: seguridad en computación dentro de una instalación pequeña.

Apéndice 5. Glosario de términos en computación.

Apéndice 6. Bibliografía complementaria.

e)
Nombre: "Computer Security Requeriments.
Guidance for applying the Department of Defense Trusted Computer System. Evaluation criteria in specific environments".
CSC-STD-003-85
Autor: Department of Defense Standard. Department of Defense.
25 de junio de 1985

Explicación sintética de cada capítulo:

Es una publicación de distribución pública ilimitada. Actualmente este documento se esta utilizando por el centro de seguridad en cómputo (DoDCSC) de los E.U.. Intenta ser usada para establecer los requerimientos de seguridad mínimos para el procesamiento, almacenamiento y recuperación de información clasificada y sensible sin importar los sistemas de procesamiento automáticos utilizados.

Esta guía contiene 4 apartados y una sección de referencias.

"Introduction". Describe el contenido de la guía. Se sostiene la idea de que este documento contiene las recomendaciones que el centro de seguridad en cómputo (DoDCSC) cree adecuadas como mínimo para tener un nivel de seguridad aceptable.

"Definitions". Compendio de definiciones y términos que se aplican en toda la guía.

"Risk index computation". Describe el paso inicial para determinar el nivel de evaluación mínimo requerido para determinar el "índice de riesgo de un sistema". Da 2 fórmulas sencillas a seguir y 2 tablas de referencia.

"Computer security requirements". Se identifican por medio de una tabla las clases apropiadas para sistemas basados en el índice de riesgo del punto 3.

"References". Referencias bibliográficas.

f)
Nombre: "Technical Rational Behind CSC-STD-003-85. Computer Security requeriments".
Guidance for applying. Trusted computer system evaluation criteria in specific environments".
Autor: Department of Defense Standard. Department of Defense.
25 de junio de 1985

Explicación sintética de cada capítulo.

Esta guía esta compuesta por cuatro capítulos, 3 apéndices, 1 glosario y una lista de acrónimos.

Capítulo 1. "Introduction". En este capítulo se plantea el ambiente de discuión que se tratará a lo largo de la guía. Plantea el que se establezca una métrica para categorizar sistemas de acuerdo a las protecciones de seguridad que se proveen e identificar la protección de seguridad mínima necesaria en ambientes particulares.

Capítulo 2. "Risk index". Discute el índice de riesgo, según definición del autor es la disparidad entre la claridad mínima o autorización de los usuarios del sistema y la sensibilidad máxima de datos procesados por el sistema.

Capítulo 3. "Computer security requirements for open security environments". Presenta una discusión de los requerimientos de seguridad para ambientes de seguridad abiertos.
Un ambiente de seguridad abierto es aquel en el cual las aplicaciones del sistema no están adecuadamente protegidas contra la presencia de lógica con mala intención. En el apéndice C se describe la lógica de mala intención y los ambientes de seguridad abierta con más detalle.

Capítulo 4. "Computer security requirements for closed security environments". Presenta una discusión de los requerimientos de seguridad para ambientes de seguridad cerrados.

Un ambiente de seguridad cerrado es aquel en el que las aplicaciones del sistema están adecuadamente protegidas contra la lógica con mala intención.

Apéndice A. "Summary of criteria". El sistema de evaluación de sistemas confiables DoD proporciona las bases de los requerimientos de seguridad y una métrica con la cual se evalúa el grado de confianza que puede ser referenciada en un sistema de cómputo. Estos criterios son jerárquicamente ordenados en una seria de clases de evaluación donde cada una de esas clases abarca una cantidad incremental de confiabilidad. Un resumen de cada clase de evaluación es presentada en este capítulo.

Apéndice B. "Detailed description of clearances and data sensitives". Descripción detallada sobre el qué son los datos sensibles.

Apéndice C. "Environment types". La cantidad de seguridad en cómputo que se necesite depende no sólo del índice de riesgo (capítulo 2) sino también de la naturaleza del ambiente. Los dos tipos de ambientes de sistemas definidos en este documento están basados en si están o no protegidos adecuadamente las aplicaciones contra la lógica de mala fe. Define ambos tipos de ambientes con más detalle. Define cuatro términos esenciales:
1.- Ambiente.
2.- Aplicación.
3.- Lógica de mala fe.
4.- Control de configuración.
Definidos esos conceptos describe qué papel ocupan en los ambientes abiertos y cerrados.

Glossary. Definiciones de muchos de los términos utilizados en este documento.

Referencias bibliográficas.

g)
Nombre: "Password management guideline".
Autor: Fort George G. Meade.
Department of defense. Computer security center.
12 de abril de 1985

Explicación sintética de cada capítulo:

Esta guía desarrollada por el Departamento de la Defensa de los E.U. consta de 4 capítulos y 6 apéndices.

Capítulo 1. "Scope". Prescribe los pasos que deben ser tomados para minimizar la *vulnerabilidad* de los passwords ante los siguientes escenarios:

Un password debe inicialmente ser asignado a un usuario por un sistema de procesamiento de datos automático.
El password de un usuario debe ser cambiado periódicamente.
El sistema de procesamiento automático de datos debe mantener un almacenamiento de los passwords (ya sea en una base de datos o en archivos).
Los usuarios deben recordar sus passwords.
Los usuarios deben escribir sus passwords en el sistema de procesamiento de datos automático en tiempo de *autenticación.*

Capítulo 2. "Control Objectives". Capítulo en el que se plantea que los sistemas que son usados para procesar o manipular información sensible o clasificada deben asegurdar las cuentas a pesar de que exista de por medio una política de seguridad obligatoria u opcional. Para asegurar la *confidencialidad* de las cuentas debe existir una entidad autorizada y competente que pueda accesar y evaluar la información de las cuentas por un medio seguro dentro de una cantidad considerable de tiempo, y sin procedimientos reforzados.

Capítulo 3. "Definitions". Un gosario de términos utilizados en todo el documento.

Capítulo 4. "Guidelines". Capítulo extenso en el que se tratan las responsabilidades de los involucrados en el uso de sistemas que utilizan passwords, por un lado el "oficial de seguridad de sistema" o conocido también como "superusuario", o "root". Y por el otro abarca las responsabilidades del usuario.
Abarca posteriormente la funcionalidad de los mecanismos de *autenticación* incluyendo el problema del almacenamiento de los passwords en alguna parte del sistema.
Finaliza con un comentario muy breve sobre algunas *vulnerabilidades* que desde siempre han existido en sistemas que utilizan passwords para permitir el acceso a sus usuarios.

Apéndice A. Es un algoritmo para la generación de passwords.

Apéndice B. Es un algoritmo de *cifrado* de passwords.

Apéndice C. Determinación de la longitud de los passwords.

Apéndice D. Bases de protección para passwords.

Apéndice E. Características para poner en práctica en aplicaciones muy sensibles.

Apéndice F. Probabilidades de adivinación de passwords.

h)
Nombre: "RFC 1244 *Site* Security Handbook".
Autores P.Holbrook & J. Reynolds.

Editorial: (Request for comments)
Julio de 1991.

Explicación sintética de cada capítulo:
Este documento esta organizado en 11 capítulos.
Capítulo 1. "Introduction". Discute los resultados derivados que un centro de cómputo esperaría si se crean políticas de seguridad. El documento no intenta forzar la selección que un centro de cómputo podría realizar ya que eso depende de las circunstancias locales. Los casos en los que sucede una eventualidad deben ser tratados de manera muy particular, aquí únicamente se dan sugerencias de acción.

Capítulo 2. "Establishing official *site* policy on computer security". Establece todo el ambiente en el cual debe pensarse para desarrollar una política de seguridad. Da algunas recomendaciones cuando las políticas son violadas.

Capítulo 3. "Establishing procedures to prevent security problems". En este capítulo se identifican varios escenarios interesantes, por ejemplo, el definir una política de seguridad permite definir qué se necesita proteger realmente.
Permite identificar posibles problemas de seguridad en el control de activos en base a costos. Abarca un poco a los que se refiere a la *seguridad física* y termina con un estudio sobre la actividad de usuarios no autorizados.

Capítulo 4. "Types of security procedures". Define 3 tipos de procedimientos de seguridad y los explica. Estos procedimientos son:
Procedimientos de administración de cuentas.
Procedimiento de administración de passwords.
Procedimiento de administración de configuración.

Capítulo 5. "Incident Handling". Da una metodología para evaluar y notificar algunos incidentes que se pudieran presentar.

Capítulo 6. "Establishing post-incident procedures". En este capítulo se enseña a que después de un incidente de seguridad no se pierda la cabeza y en vez de ello se piense en tomar las medidas más prudentes que evitarán que en posteriores ocasiones se vuelvan a producir, al autor recomienda que se tome nota de todo el ambiente cuando ocurrió el incidente para ir minimizando las *vulnerabilidades*, y si es necesario actualizar las políticas o procedimientos de seguridad si es que se detectó algo no identificado y que provocó el incidente.

Capítulo 7. "References". Bibliografía.

Capítulo 8. "Annotated bibliography". Bibliografía.

B) Libros de lectura ligera.

Los libros que se encuentran en este rubro son libros cuyo contenido general no sirve del todo para ser retomado en este trabajo y únicamente la lectura de algún capítulo sí lo es.

a)
Nombre: "Sistemas de autentificación para seguridad en redes".
Autor: Rolf Opplieger.
Editorial: Computer Ra-Ma
Edición 1996.
ISBN: 958-682-081-5
Url: http://www.alfaomega.com.mx

Explicación sintética de los capítulos leídos.
La estructura general de este libro se basa en enfocarse en cada capítulo en un sistema concreto de *autenticación* y de distribución de *llaves*, dedicando secciones separadas a resumir su desarrollo, revisar su arquitectura y describir y discutir los protocolos criptográficos que implementa. El libro consta de 9 capítulos, un apéndice, un glosario y una lista de abreviaturas y acrónimos.
Los capítulos referidos para efectos de este trabajo son 2:

Capítulo 1. "Introducción". Presenta las razones para el uso de los sistemas de *autenticación* y de distribución de *llaves* en entornos distribuidos y de red. Abarca la terminología de la arquitectura de seguridad *OSI* incluyendo una descripción de los servicios y mecanismos de seguridad.

Capítulo 8. "Comparación". Realiza una comparación funcional de los protocolos presentados en el contenido del libro. Abarca sistemas de *autenticación* y de distribución de *llaves*. Hace una comparación de los *servicios de seguridad*, técnicas criptográficas, estandarización, disponibilidad y posibilidad de exportación.

b)
Nombre: "*Firewalls* y la seguridad en internet".
Autor: A Simon & Schuster Company.
Editorial: Prentice Hall.
Segunda edición 1996.
ISBN: 968-880-806-7
Url: http://www.prentice.com.mx

Explicación sintética del o los capítulos leídos:
Este libro esta destinado para los administradores de sistemas que perciben los riesgos implicados en la conexión de un sistema de cómputo a internet. Cuando se conecta una

red LAN (como la de *D.G.S.C.A.* o la de *D.C.A.A.*) a internet se permite que los usuarios lleguen al mundo exterior y se comuniquen con él. Al mismo tiempo se permite que el mundo exterior llegue a la LAN interna al centro de cómputo e interactúe con ella. Los *firewalls*, en el sentido estricto, son ruteadores a través de los cuales fluye el *tráfico* de datos. Si algún intruso trata de tener un acceso no autorizado a la red, el *firewall* puede detenerlo y no permite adentrarse a los sistemas del centro de cómputo.
Los capítulos referidos para efectos de este trabajo son 2, y el apéndice B.

Capítulo 2. "Seguridad". En todo el mundo, todos los días se producen entradas no autorizadas y violaciones de la seguridad. Estos violadores no son sólo los *intrusos* de internet, sino también los empleados de la oficina de al lado, que roban tiempo de computadora y servicios para su uso personal o para fines mal intencionados.
En este capítulo se examina en detalle la seguridad de las computadoras. Se puede tener un concepto claro de qué es la seguridad, cómo se puede proteger contra abusos y de qué medios se dispone para ayudar en esas tareas. Debido a que *Unix* es el sistema predominante este capítulo se centra en él.
En este capítulo se tratan los siguientes tópicos: Análisis de los niveles de seguridad según el "*orange book*" y de la seguridad canadiense; Análisis de cuestiones de seguridad local; Contraseñas; Cómputo confiable; Comprensión de permisos; Exploración de métodos de *cifrado* de datos e *IP Spoofing*.

Capítulo 3. "Cómo diseñar una política de Red". Busca los preparativos para conectar una red LAN a internet, define cuáles recursos y servicios de la red se desean proteger. La política de red es un documento que describe los intereses de seguridad de red de una organización.
Este capítulo aborda los pasos a seguir para diseñar una política de red. Entre las cuestiones que se exploran esta la planeación general de seguridad de la red, la política de seguridad del sitio y el *análisis de riesgos*. También aborda la identificación de recursos y amenazas, el uso y las responsabilidades de red y los planes de acción en caso de que sea violada la política de seguridad. Con esto pasos se ayuda a monitorear el uso de los sistemas, los mecanismos y horarios; asimismo, cubre los procedimientos de administración de cuentas y configuración y los de recuperación. Por último, este capítulo analiza el uso del *cifrado* de datos para proteger la red, el uso de los sistemas de *autenticación*, listas de correo, grupos de noticias y los equipos de respuesta de seguridad.

Apéndice B. "Fuentes de información". Recomendaciones que hace el autor para proteger los sistemas y datos. En esta sección se encuentran muchas direcciones en internet en donde se pueden obtener códigos fuentes y ejecutables que detectan varias *vulnerabilidades* de sistemas con la finalidad de cuestionar si la seguridad de los equipos en los que se ejecutan dichos programas son confiables o no lo son. Generalmente son programas hechos para ejecutarse con *unix*.

c)

Nombre: "Trusted Computer System Evaluation Criteria (*orange book*)".
Autor: Department of Defense Standard. Department of Defense.
December 1985

Explicación sintética del tópico leído.
De acuerdo con las normas de seguridad establecidas por el Departamento de la Defensa de los Estados Unidos, los criterios estándar de evaluación de computadoras confiables, conocidos como "*orange book*"[14], usan varios niveles de seguridad para proteger de *ataques* al hardware, al software y a la información almacenada. Estos niveles se refieren a diferentes tipos de *seguridad física, autenticación* de usuario, confiabilidad del software del sistema operativo y de aplicaciones de usuario. Estos estándares también imponen límites a los sistemas que puedan conectarse a los nuestros.
Enseguida se describen cada uno de los niveles declarados en el *Orange book*:

Nivel D1: El nivel D1 es la forma más baja de seguridad. Esta norma establece que el sistema entero no es confiable. No se dispone de protección para el hardware; el sistema operativo se compromete fácilmente y no existe *autenticación* respecto de los usuarios y sus derechos a tener acceso a la información almacenada en la computadora. Este nivel de seguridad por lo general se refiere a los sistemas operativos como MS-DOS, MS-Windows y el sistema 7.x de Apple de Macintosh.

Nivel C1. El nivel C tiene dos subniveles de seguridad: el C1 y el C2. El nivel C1, Sistemas de Protección de Seguridad Discrecional, se refiere a la seguridad disponible en un sistema *Unix* típico. Existe cierto nivel de protección para el hardware, ya que éste no puede comprometerse fácilmente, aunque es posible. Los usuarios deben identificarse ante el sistema mediante su login y su contraseña. Se emplea esta combinación para determinar los derechos de acceso a programas e información que tiene cada usuario.
Estos derechos de acceso son los permisos de archivo y de directorio. Los controles de acceso discrecional permiten al dueño del archivo o directorio, así como al administrador del sistema, evitar que ciertas personas o grupos tengan acceso a dichos programas o información. Sin embargo no se impide que la cuenta del administrador del sistema realice ninguna actividad. En consecuencia, un administrador poco escrupuloso puede comprometer fácilmente la seguridad del sistema sin que nadie lo sepa.
Además, muchas de las tareas cotidianas de administración del sistema sólo pueden ser realizadas por el login del usuario llamado raíz (root). Con la actual descentralización de los sistemas de cómputo, no es raro que en una organización encontremos dos o tres personas que conocen la contraseña del superusuario. Esto es en sí un problema, pues no hay forma de distinguir entre los cambios que hicieron ayer Hansel o Gretel.

[14] El libro naranja ha permanecido sin cambios desde que se adoptó como estándar del Departamento de la Defensa en 1985. Durante muchos años ha constituido el método básico para evaluar la seguridad de sistemas operativos multiusuarios en mainframes y minicomputadoras. Otros subsistemas, como las bases de datos y las redes de computadoras, han sido evaluados mediante las interpretaciones del libro naranja, como la interpretación de Bases de datos confiables y la interpretación de redes confiables.

Nivel C2.
El segundo subnivel, C2, esta diseñado para ayudar a resolver los problemas anteriores. Además de las funciones del C1, el nivel C2 cuenta con las características adicionales que crean un ambiente de acceso controlado. Este ambiente tiene la capacidad de restringir aún más el que los usuarios ejecuten ciertos comandos o tengan acceso a ciertos archivos, con base no solo en los permisos, sino también en los niveles de autorización. Además este nivel de seguridad requiere que se audite el sistema, lo cual implica registrar una auditoria por cada acción que ocurra en el sistema.
La auditoria se utiliza para llevar registro de todas las acciones relacionadas con la seguridad, como pueden ser las actividades efectuadas por el administrador del sistema. La auditoria requiere de *autenticación* adicional pues, sin ésta, ¿cómo estar seguros de que la persona que ejecuta el comando realmente es quien dice ser?. La desventaja de la auditoria es que requiere recursos adicionales del procesador y del subsistema de disco.
Con el uso de autorizaciones, es posible que los usuarios de un sistema C2 tengan la autorización para realizar tareas de administración de sistema sin necesidad de la contraseña de root. Esto permite llevar mejor cuenta de las tareas relacionadas con la administración del sistema, ya que es cada usuario quien ejecuta el trabajo y no el administrador del sistema.
No deben confundirse estas autorizaciones adicionales con los permisos SGID y SUD que pueden aplicarse a un programa. Más bien se trata de autorizaciones específicas que permiten al usuario ejecutar comandos específicos o tener acceso a ciertas tablas de acceso restringido. Por ejemplo, cuando ejecutan el comando ps, los usuarios que no tienen autorización de ver la tabla de procesos sólo verán sus propios procesos.

Nivel B1. El nivel de seguridad B consta de tres niveles. El nivel B1, llamada "protección de seguridad etiquetada", es el primer nivel con soporte para seguridad multinivel, como el secreto y el utlrasecreto. En este nivel se establece que el dueño del archivo no puede modificar los permisos de un objeto que esté bajo *control de acceso* obligatorio.

Nivel B2. El nivel B2, conocido como "protección estructurada", requiere que todos los objetos estén etiquetados. Los dispositivos como discos, cintas y terminales, pueden tener asignado uno o varios niveles de seguridad. Este es el primer nivel en el que se aborda el problema de la comunicación de un objeto con otro que se encuentra en un nivel de seguridad inferior.

Nivel B3. El nivel B3, llamado de "dominios de seguridad", refuerza los dominios con la instalación de hardware. Por ejemplo, se utiliza hardware de manejo de memoria para proteger el dominio de seguridad contra accesos no autorizados y modificaciones de objetos en diferentes dominios de seguridad. Este nivel requiere también que la terminal del usuario este conectada al sistema a través de una ruta de acceso confiable.

Nivel A. El nivel A, conocido como de "diseño verificado", constituye el nivel de seguridad validada más alto en todo el libro naranja. Cuenta con todo un proceso estricto de diseño, control y verificación. Para alcanzar este nivel de seguridad, deben incluirse todos los componentes de los niveles inferiores; el diseño debe verificarse

matemáticamente, y debe realizarse un análisis de los canales cubiertos y de distribución confiable. La distribución confiable significa que el hardware y el software hayan estado protegidos durante su traslado para evitar violaciones de los sistemas de seguridad.

C) Libros de lectura rápida.

Son libros que únicamente se retoma algún tema que pudiera tratarse en el trabajo de tesis.

a)
Nombre: "Seguridad y comercio en el Web. Riesgos, tecnologías y estrategias."
Autor: Simson Garfinkel y Gene Spafford.
Editorial: Mc Graw Hill and O'Reilly.
Edición junio de 1999.
ISBN: 1-56592-269-7

Explicación sintética del tópico leído.
Este libro se divide en siete partes, incluye 49 capítulos y cinco apéndices.
Los tópicos leídos fueron tomados de todos los capítulos, ellos son:
El problema de la seguridad en el Web (capítulo 1). El problema de la seguridad de las computadoras que se encuentran conectadas a internet son 3:
Asegurar que el servidor y los datos que contiene estén disponibles.
Asegurar la información que viaja entre los procesos servidores y los procesos clientes.
Asegurar la computadora del usuario.
Administración de riesgos (capítulo I). Entre más medidas de seguridad se utilicen, más se reduce el riesgo. La meta debe ser reducir el riesgo tanto como sea práctico (y se pueda pagar), para luego tomar medidas adicionales de forma que, en caso de ocurrir un incidente de seguridad, sea posible una rápida recuperación.
Ataques de negación de servicio (capítulo III). Sucede cuando un usuario o programa consume tal cantidad de un recurso compartido que no deja nada para otros usuarios o usos.
Máquinas históricamente inseguras (capítulo XIII). Dato curioso, la mayoría de los problemas identificados por el autor del RFC No. 602, Metcalfe en 1973 perduran hasta nuestros días.
Principales problemas de seguridad de as máquinas hoy en día (capítulo XIII). Atención especial al hacking.
Cómo reducir el riesgo minimizando servicios (capítulo XIII).
Seguridad física (capítulo XIII). Habla además de cómo elaborar un plan de *seguridad física*.

D) Libros de lectura superficial.

Son libros de los que se retoma únicamente algún concepto.

a)
Nombre: "Java Cryptography"
Autor: Jonathan Knudsen
Editorial: O'Reilly.
Primer edición mayo de 1998.
ISBN: 1-56592-402-9

Explicación sintética del tópico leído:
Este libro esta organizado como un "sandwich". Los capítulos externos 1,2 y 12 proporcionan el contexto del resto del libro. De los capítulo 3 al 11 contienen descripciones pragmáticas[15] y metódicas de técnicas criptográficas generales (implementadas en Java) incluyendo algunos ejemplos.
Conceptos retomados:
Capítulo 1. "Introducción". Describe el papel de la criptografía en el desarrollo de sistemas seguros e introduce algunos ejemplos cortos de programación utilizando criptografía.
Conceptos retomados de este capítulo: Sistema seguro, criptografía, seguridad de las plataformas.

Capítulo 2. "Conceptos". Introduce los conceptos fundamentales de la criptografía: *cifrados*, resúmenes de mensajes, firmas. Introduce otros conceptos de importancia en este trabajo tales como *confidencialidad*, *integridad* y *autenticación*.

Capítulo 6. "*Autenticación*". Indica cómo se usan los resúmenes de mensajes, firmas y certificados para implementarse en mecanismos de *autenticación*.

Capítulo 7. "*Cifrado* de datos". Cubre *cifrados* simétricos y asimétricos. Modos de cifrar y sistemas híbridos.

[15] Pragmatico. Perteneciente o relativo al pragmatismo. Pragmatismo.- Método filosófico, divulgado principalmente por el psicólogo norteamericano William James, según el cual el único criterio válido para juzgar de la verdad de toda doctrina científica, moral o religiosa, se ha de fundar en sus efectos prácticos.

2.3. Tesis.

a)
"Protocolos criptográficos de *autenticación* e intercambio de *llaves* basados en passwords".
Leobardo Hernández Audelo.
Mayo de 1999.
Maestro en ciencias de la computación.
Universidad Nacional Autónoma de México.
Unidad Académica de los Ciclos Profesional y de Postgrado I.I.M.A.S.
La tesis fue préstamo personal del autor.
Dirección de correo electrónico del autor: leo@servidor.unam.mx

b)
"An analysis of security incidents on the internet 1989 – 1995"
John D. Howard
Abril 7 de 1997
Doctor de Filosofía en ingeniería y política pública.
Carnegie Mellon University
Pittsburg, Pennsylvania USA.
Tesis obtenida del url: http://www.cert.org/research/JHThesis [16]

2.4. Hemeroteca.

A. Periódicos.

a)
Humanidades.
Artículo leído: La tecnología y el robo de datos.
Autor del artículo: Marco A. MurrayLasso
Facultad de Ingeniería de la UNAM.
Comentario sobre el artículo: En este artículo el autor da una visión particular sobre lo que es hoy en día el robo de datos realizados de manera muy elaborada. Según el autor en Alemania se puede obtener un scanner por 80 dólares con el que se puede escuchar cualquier llamada telefónica analógica inalámbrica que se haga en un radio dado. Los espías industriales interceptan llamadas telefónicas y faxes. Los atacantes computacionales espían claves secretas y números de tarjetas de crédito. Los gobiernos sistemáticamente monitorean sistemas de comunicación.
El paradigma de "trabajar en casa" quizá ya no sea una buena idea ya que la *vulnerabilidad* de las comunicaciones es muy alta, con 7,400 dólares se pueden penetrar eslabones inter-

[16] Enlace visitado el día 10 de marzo del 2000

satelitales. Con 2,400 dólares se pueden penetrar comunicaciones por radio direccional. La solución a todos estos problemas sigue siendo una: el *cifrado* de los datos.

b)
Medios. Suplemento de "El Nacional"
Directora General: Enriqueta Cabrera.
Domingo 7 de julio de 1998.
Artículo leído: Reflexiones sobre el derecho a la *privacidad*.
Autor: Ernesto Villanueva.
Comentario sobre el artículo:

El derecho a la *privacidad* o a la intimidad forma parte de las áreas de estudio del derecho de la información que han sido poco abordadas en México, como otros rubros relacionados. Ello no es sorprendente si se toma en cuenta que la bibliografía mexicana sobre el tema es casi inexistente, salvo excepcionales artículos o apartados de obras. Se trata por supuesto, de una asignatura relevante en la vida contemporánea, sobre todo por el rápido desarrollo tecnológico que permite intrusiones eventualmente ilegítimas en el ámbito de la *privacidad* personal, además de los añejos rezagos que México muestra en la materia.
No esta por demás recordar que la única excepción permisible en el derecho comprado para afectar el derecho a la *privacidad* es la existencia del interés público preeminente. Y una información de interés público es aquella que contribuye a materializar el derecho del ciudadano a estar informado, a efecto de que participe de mejor manera en los asuntos públicos. A contrario sensu, la información que únicamente satisface la curiosidad, el morbo o apela al sensacionalismo no puede considerarse de interés público, en virtud de que su presencia no ofrece más o mejores elementos de juicio para hacer de la noción de ciudadanía una premisa verificable.
Los mecanismos jurídicos de protección a la *privacidad* en México observan limitaciones importantes a la luz de las razones siguientes:

Si bien es cierto que el artículo 7 de la Constitución prevé el derecho a la *privacidad* como límite de la libertad de información (y, en forma complementaria, el artículo 16, fracción primera de la Carta Magna es igualmente aplicable) también lo es que no ofrece en ningún momento un concepto más o menos razonable del significado de vida privada o *privacidad*, lo que demanda un ejercicio de interpretación jurídica.
La Suprema Corte de Justicia de la Nación tampoco ha resuelto con solvencia el vacío conceptual sobre el concepto de vida privada, pues al respecto ha sostenido en tesis de jurisprudencia que "la ley no da un concepto de vida privada de una manera explícita, pero si puede decirse que lo contiene implícito, toda vez que en los artículos siguientes se refiere a los *ataques* a la Nación Mexicana, a las entidades políticas que la forman, a las entidades del país y a la sociedad. Para determinar lo que es la vida privada puede acudirse al método de la exclusión y sostener que vida privada es aquella que no constituye vida pública".

Si bien la Ley de imprenta –expedida con anterioridad el inicio de la vigencia de la Constitución de 1917- establece en el artículo 1 cuatro causales que constituyen *ataques* a la vida privada, habría que señalar que se trata de hipótesis normativas que, por un lado, confunden el derecho a la *privacidad* con el derecho al honor y a la propia imagen, los cuales están también protegidos en el Código Penal bajo los tipos de calumnia y difamación, y en el Código Civil en la figura del daño moral. Por otra parte, muestran términos de corte autoritario, que no reflejan la circunstancia histórica de fin de siglo y de milenio, que tienen impregnadas las improntas de la intolerancia, de la pluralidad y de la diversidad.
No existen en México normas expeditas para hacer valer el derecho a la *privacidad* con cierta eficacia disuasoria en virtud de que, por un lado, se puede advertir una reducida experiencia judicial en el tratamiento de estos casos, circunstancia que genera procesos judiciales largos, costosos e imprácticos, y, por otro, las sanciones aplicables (en particular la prevista en la Ley de imprenta) tienen más bien un cometido simbólico.

2.5. Seminarios (conferencias)

Disertación científica sin pruebas, manifestación de experiencias.

a)
"Mecanismos de *autenticación* de usuarios".
Organizador: Dirección de cómputo para la investigación. Unidad de investigación en cómputo aplicado de la *D.G.S.C.A.*
Fecha de realización: 26 de junio de 1998
Expositor: Dr. Enrique Daltabuit Godas.
Moderador:
Material: Conferencia impresa.
Comentario sobre el seminario: *Autenticación* es un proceso para verificar un reclamo de identidad entre dos partes. *Autenticación* basada en passwords significa que las partes, previamente a la ejecución del protocolo, acuerdan un password p, cuyo conocimiento sirve para que una parte demuestre su identidad a la otra.
Los esquemas convencionales basados en passwords involucran secretos invariantes con respecto al tiempo, y funcionan de la siguiente manera. Una parte A, debe, de alguna manera, probar a otra parte B que conoce P, revelando P mismo y demostrando así ser quien dice ser. Es posible mejorar este método haciendo que A revele una función h(p), difícil de invertir (tipo hash) en lugar de P, y entonces B verifica que h(p) corresponda al secreto asociado a A. De esta manera no es necesario transmitir P en claro sobre la red, y además, B no necesita guardar P sino h(p). También es posible realizar variantes de estas posibilidades. Estos son los esquemas típicos de la mayoría de los sistemas que basan su proceso de *autenticación* en passwords. Este es el caso del sistema operativo *UNIX*.

Lo anterior se conoce como *autenticación* débil porque se basa directamente en un password (o hash de este) que un usuario selecciona y memoriza. El password así escogido es relativamente pequeño, y además, usualmente, basado en una palabra o variante de una palabra fácil de memorizar. Por lo tanto, es criptográficamente débil susceptible de ser atacado por medio de *ataques* conocidos como "*ataques* diccionario".
Si el secreto que A conoce tiene las deficiencias descritas, entonces parecerá imposible utilizarlo para lograr un protocolo de *autenticación* fuerte. Sin embargo, a principios de los 90's se descubrió que el problema sí tiene solución y a la fecha existen varias alternativas de solución. Entre estas alternativas están los protocolos conocidos como *LGSN*.
Tales protocolos se conocen como criptográficos en el sentido que realizan alguna técnica criptográfica para lograr sus objetivos de seguridad. También existe otra corriente de soluciones alternas que no utiliza criptografía sino más bien relaciones matemáticas y técnicas de conocimiento cero. Entre estos últimos están los protocolos OKE, SRP, S3P entre otros.
Debido a la relativa juventud de estas soluciones y a las resistencias históricas de las grandes compañías de software, actualmente no se han implementado de forma masiva en los esquemas de *autenticación* de los distintos sistemas en diversos ámbitos de la aplicación. No obstante, empiezan a aparecer recomendaciones para implementar este tipo de protocolos en sistemas específicos para superar problemas de seguridad asociados a la *autenticación* segura basada en pequeños secretos.

b)
"RSA vs CCE"
Organizador: Dirección de cómputo para la investigación. Unidad de investigación en cómputo aplicado de la *DGSCA*.
Fecha de realización: 26 de junio de 1998
Expositor: José de Jesús Angel Angel. SeguriDATA
Moderador:
Material: Conferencia impresa.
Comentario sobre el seminario: El componente fundamental de un sistema de *cifrado* es el procedimiento bajo el cual se realiza el *cifrado* y des*cifrado* de información. Tal procedimiento se basa en los llamados algoritmos de *cifrado*. La platica se centró en una comparativa entre ambos algoritmos en relación a: seguridad, confiabilidad, eficiencia, sencillez y en la independencia de la plataforma de cómputo.
La conferencia estuvo cargada de muchos conceptos técnicos y matemáticos.

2.6. Congresos.

Reunión de muchos expositores para analizar diversos temas afines.

a)
Organizador: UNAM, SEP, ISOCMex, ITESM, INEGI, ILCE, SOMECE, ANIEI, Centro de investigación en cómputo, TecnoMed, CFE, Cómputo Académico UNAM.
Fecha de realización: Octubre de 1998
Expositores: Ariel Futoransky y Emiliano Kargieman
"Técnicas avanzadas de Auditoria".
Material: Memoria. Conferencia impresa.
Comentario sobre la conferencia: La conferencia giró en torno a una técnica criptográfica basada en funciones hash para el control de bitácoras en aplicaciones y mostró como podría implementarse en sistemas tan comunes como lo son los sistemas de la compañía microsoft.

b)
Organizador: UNAM, SEP, ISOCMex, ITESM, INEGI, ILCE, SOMECE, ANIEI, Centro de investigación en cómputo, TecnoMed, CFE, Cómputo Académico UNAM.
Fecha de realización: Octubre de 1998.
Expositores: Ariel Futoransky y Emiliano Kargieman.
"Conjeturas inválidas en el diseño e implementación de protocolos criptográficos"
Material: Memoria. Conferencia impresa.
Comentario sobre la conferencia: Mostró que aún un sistema tan mundialmente utilizado y reconocido como "seguro" es atacable dejando ver cierta información sensible durante la transmisión. [17]

c)
"Integrando soluciones de seguridad: Retos y experiencias"
Fecha de realización: 6 de octubre de 1999.
Expositores: Sergio Avila y Ernesto Ordoñez.
Institución: SGI, Red UNO, México
Organizador: Congreso General de Cómputo UNAM.
Material: Conferencia impresa.
Comentario sobre el seminario: Hoy en día la seguridad en redes ha dejado de ser un tema de investigación académica o ambientes militares, para convertirse en una necesidad de todas las organizaciones conectadas a Internet.
Un boom de *ataques* a páginas de web y a otros sistemas ha despertado, como con un balde de agua fría, a diversas empresas e instituciones mexicanas.
Los productos de seguridad que se venían cocinando desde hace ya algunos años, están empezando a ver un mercado creciente, especialmente en México.
Actualmente, existen muchos productos de seguridad. Todos con sus ventajas y desventajas, y cada producto se adecua mejor a ciertos ambientes, según las necesidades.
El objetivo de esta conferencia es compartir con el público las experiencias que han tenido los autores en la integración de diversos productos de seguridad, qué estrategias y

[17] Estos conferencistas fueron los primeros a nivel mundial en encontrar una *vulnerabilidad* en el *shell* denominado "secure *shell*".

metodologías han utilizado, qué dificultades se han presentado y cuáles son los retos para el futuro inmediato.
No es objetivo de esta presentación el comparar los productos, sino el describirlos y el especificar cuándo, cómo y por qué utilizarlos.

d)
"Técnicas de hacking"
Fecha de realización: 7 de octubre de 1999.
Expositor: Ing. Angel Peña Angeles e-mal: angel@miditel.com.mx
Institución: IPN
Organizador: Congreso General de Cómputo UNAM.
Material: Disponible en CDROM en las memorias de la conferencia.
Comentario sobre el seminario: Se comentaron de manera general las técnicas más usuales que los *Hackers* aplican para la invasión en los diferentes sistemas de Computo y comunicaciones.
En el medio de la informática es muy común escuchar acerca de los *Hackers*, pero, cuáles son sus técnicas más comunes y como es que se introducen en nuestros sistemas y aplicaciones de computo.
Las operaciones de invasión, se realizan en los equipos de comunicaciones, Plataformas Operativas de Servidores, aplicaciones como el correo electrónico, o el web hosting, incluso en aplicaciones como el chat. Se describieron en forma global los pasos de invasión ejecutados por un *Hacker* para realizar hacking en:

- Scan
- Sniff
- *Spoof*
- Hijack
- Hack sobre ICQ y mIRC

2.7. Mesas redondas.

Reunión de expositores con experiencias en el tema para debatir sobre él.

a)
El día 10 de agosto del 2000 se llevó a cabo una mesa redonda en la Facultad de Contaduría y administración. Este trabajo fue motivo de charla por unos instantes.

2.8. Internet.

A. URL's.

a)
Boletín del criptonomicon.
http://www.IEC.csic.es/criptonomicon [18]
Comentario: Se cuenta con los 59 números de la revista electrónica "criptonomicon" la cual se encarga de la difusión práctica para preservar la *confidencialidad*, *integridad*, y seguridad de los datos alojados en las computadoras con herramientas generalmente de índole gratuita. En muchas de las ocasiones esta revista electrónica es realizada en mancuerna con investigadores de todo el mundo y *hackers* que de manera desinteresada participan redactando algún articulo o alguna novedad sobre los *ataques* que realizan y detallan la manera en cómo hacerlos.

b)
Risk And Risk Analysis
Impresión de documento localizado en:
http://www.sevenlocks.com/papers/PapersRiskAnalysis.htm [19]
Comentario: Uno de los mejores sitios que hablan sobre el *análisis de riesgos* en materia de cómputo. En este enlace se puede obtener una clasificación bastante interesante sobre los distintos riesgos de cómputo, además para cada uno de éstos se da su afectación, el nivel de prevención, nivel de detección, frecuencia con la que se da y el nivel de daño que podría llegar a producir si es que se presentase el riesgos en cuestión. También discute la psicología de la valoración de riesgos e intenta inventar una ciencia para ella. Contiene algunas gráficas muy ilustrativas sobre el porcentaje de sitios que no tienen absolutamente ningún plan de seguridad, empresas que no cuentan con planes de recuperación de desastres, etc. Además contiene un apartado donde resume 23 herramientas que se encuentran en el mercado norteamericano que ayudan a realizar *análisis de riesgos*.

c)
http://www.cnie.org/nle/rsk-11.html [20]
Comentario: Excelente sitio en donde se describe la manera en cómo debe desarrollarse un *análisis de riesgos*.

d)
http://catless.ncl.ac.uk/Risks [21]
Comentario: Uno de los foros más completos sobre riesgos en sistemas y computo en general. Tiene actualmente 20 volúmenes públicos de trabajos realizados en línea.

[18] Enlace visitado el dia 2 de abril del 2000.
[19] Enlace visitado el dia 5 de octubre de 1999.
[20] Enlace visitado el dia 20 de marzo del 2000.
[21] Enlace visitado el dia 22 de febrero del 2000.

e)
http://www.technotronic.com/denial.html [22]
Comentario: Un enlace donde se encuentran varias categorías relacionadas a *ataques* en cómputo con énfasis especial a los *ataques* de tipo "Negación de servicio). Contiene incluso varios códigos fuentes escritos en lenguaje C para perpetuar *ataques*.

f)
http://www.asc.unam.mx [23]
Comentario: Aquí se puede encontrar información sobre temas específicos relacionados con la Seguridad en Cómputo y sobre las actividades que realiza el área de seguridad en cómputo de la *D.G.S.C.A.*.

B. Listas de correo a las que el autor esta actualmente inscrito:

a)
mx-seguridad-request@asc.unam.mx
Lista de seguridad en cómputo administrada por la UNAM-ASC

b)
[redacted]
Dentro de esta lista se discuten diversos tópicos relativos a los principios de una cultura de una buena administración y seguridad en los equipos *UNIX*

c)
[redacted]
Dentro de esta lista se discuten diversos tópicos relativos a los *virus* informáticos que afectan los sistemas de computo.

2.9. Centro de información o centro de Informática.

Actualmente pidiendo apoyo a 2 centros de cómputo:
- La Dirección de Cómputo para la Administración Académica (*D.C.A.A.*) y a
- La Dirección General de Servicios de Cómputo Académico.

[22] Enlace visitado el día 20 de febrero del 2000.
[23] Enlace visitado el día 22 de febrero del 2000.

2.10. Observación.

Cualquier persona y/u organización esta expuesta a una serie de riesgos derivados de factores tanto propios de sus actividades como aquellos que existen en el ambiente que los rodea, tan variables como el personal, su situación económica, la asignación de recursos financieros, la tecnología utilizada, etc.

Los equipos de cómputo en donde se procesa la información están sujetos al riesgo de que ocurra alguna eventualidad que los dañe. El no considerar los posibles riesgos que afecten al centro de cómputo, causa un costo por asumir la eventualidad, y en algunos casos la reparación del equipo o la reposición no es suficiente, tal como sucedió en los siguientes escenarios:

Miércoles 1 de julio de 1998 una explosión en un edificio de estudios bioquímicos en *Ciudad universitaria* produjo distintos daños valuados en miles de pesos.
Durante mi período de becario en la *D.C.A.A.* se dieron varios incidentes de robo de dispositivos, consumibles, periféricos incluso, en una ocasión fue extraída una computadora portátil.
En el primer trimestre de 1997 un becario activó de manera accidental una alarma contra incendios en la Dirección de Cómputo para la Administración Académica provocando algunos percances que afortunadamente no pasaron a mayores, sin embargo el costo por recargar unos tanques de gas fue de varios miles de pesos).
El más reciente caso en el que las computadoras junto con la información contenida en ellas fue extraída de la Dirección General de Bibliotecas de la UNAM como resultados de varios meses de huelga

Los daños generados son reparables en mobiliario, en equipo y en instalaciones, pero no en la información que ahí existe. En el caso de la explosión en el edificio de estudios bioquímicos se perdió una cantidad considerable de horas-hombre en investigación y documentos derivados de estudios sobre varias enfermedades, nunca se creó un plan de seguridad para la información, se reconoció de manera pública que jamás se hizo un plan de respaldo.

En el tercer escenario se pararon las actividades por lo menos durante 5 horas, todo el edificio fue evacuado, afectando con ello todas las actividades del Instituto de Investigación en Matemáticas Aplicadas y en Sistemas. Se dieron casos de histeria, miedo, incertidumbre y lo más grave de este caso es que comenzó a expulsarse un tipo de gas que elimina el oxigeno del aire cuando aun existían personas adentro del inmueble.

Los otros dos escenarios constituyen casos más extremos, tanto la información como las computadoras se perdieron, dispositivos periféricos, medios de almacenamiento (con más información) ya no fueron recuperados.

2.11 Conclusiones al segundo capítulo.

Existe demasiada información relacionada con los distintos tipos de riesgos en materia de cómputo, los libros nacionales están muy vacíos en contenidos. Nuevamente los libros con mejor contenido tanto en cantidad como en calidad son las tesis. Las referencias bibliográficas del gobierno norteamericano son muy puntuales y sirven únicamente para referenciar determinado nivel de servicio. Las platicas (conferencias, congresos, etc.) son un muy buen medio para conocer el punto de vista presencial de los asistentes y de los expertos del tema en tiempos reducidos.

Generalmente, la información se puede encontrar en tópicos muy básicos y en otras referencias bibliográficas los tópicos no están muy bien organizados. La información con mejor calidad que pudiera servir para continuar un trabajo a partir de este, podría tomarse de los trabajos elaborados por investigadores y de aquel material elaborado por gente experta en el tema como podría tratarse de los trabajos elaborados por las fuerzas armadas de los Estados Unidos.

Existen ya varias publicaciones cuyos títulos son muy sugerentes, pero en realidad están llenas de conceptos básicos o poco prácticos. Los libros de origen español tampoco son muy recomendados. La información que pudiera encontrarse en revistas de circulación popular es muy oportuna solo en el momento en el que la publicación es realizada, después, en muy pocos días, será muy común y perderá rápidamente su valor.

Nuevamente, internet pareciera ser el mejor lugar para encontrar la mejor (y la peor) información. Utilizándose de la manera adecuada puede servir incluso para mantener contacto con algunas personalidades que se dedican a riesgos computacionales.[24]

El cómputo se ve modificado cotidianamente, el día de hoy podría suceder un nuevo tipo de *ataque*, un nuevo *virus*, una nueva técnica criptoanalítica que rompa una *llave* en unas cuantas horas, todo ello sólo podría conocerse tan rápido y tan oportunamente únicamente por internet, si esperásemos a que se publicara un libro con alguna recomendación o solución entonces ya no tendría mucho valor pues internet tal vez hoy mismo publique toda la información relacionada con esa inseguridad.

[24] Como sucede con Ariel Futoransky y Emiliano Kargieman con quienes se ha establecido contacto vía correo electrónico, además de usar el mismo medio con otras personalidades académicas nacionales.

2.12. Referencia bibliográfica.

Diccionario Enciclopédico Hachette Castell
Roberto Castell.
ISBN 84.7489-160-4
Impreso en españa.
Ediciones Castell 1981.
Tomo 9

III. MARCO CONCEPTUAL.

3.1. Una definición formal de seguridad en cómputo.

El desarrollo de una terminología satisfactoria y el de una serie de principios de clasificación (*taxonomía*) son dos de los prerequisitos necesarios para los estudios sistemáticos en cualquier campo de la investigación [1]. El desarrollo de una *taxonomía* comprensiva en el campo de seguridad en cómputo ha sido un problema de interés cada vez mayor [2]. Cada vez que hay un avance parcial en esta área se reconoce como un esfuerzo altamente valuable.

El primer paso en el desarrollo de una *taxonomía* comprensiva para la clasificación de *ataques* e incidentes a la seguridad de computadoras y de redes es definir "seguridad de cómputo". Enseguida se examinaran las definiciones genéricas de seguridad en cómputo y después se tratara de particularizar un poco en otras definiciones hasta llegar a la siguiente definición formal: "la seguridad en cómputo es prevenir que los atacantes lleven a cabo sus objetivos a través de accesos no autorizados o usos no autorizados de computadoras y redes". Esta definición formal proporciona un buen límite al campo de la seguridad en computadoras y redes de computadoras y servirá para generar la *taxonomía* que se describirá mas adelante.

3.1.1 Definiciones de seguridad en cómputo simples.

En los inicios del cómputo, la seguridad en este campo implicaba muy poca o nula preocupación. El número de computadoras y el número de personas con acceso a ellas eran limitados [3,2]. El primer problema de seguridad en cómputo surgió en los inicios de los años 50's cuando las computadoras comenzaron a ser utilizadas para clasificar la información. La *confidencialidad* (también llamada *privacidad*) fue la preocupación en seguridad primaria [4] y las amenazas primarias fueron el espionaje y la invasión de la *privacidad*. En ese momento, y desde entonces hasta nuestros días la seguridad en cómputo es un problema militar prioritario en muchas naciones, el cual es visto como un sinónimo de seguridad de la información. Desde esta perspectiva, la seguridad es obtenida protegiendo la información por sí misma.

En los años iniciales de la década de los 60's, la filosofía de la compartición de recursos en cómputo y la información, ya sea dentro de una computadora como a través de una red presentaron serios problemas de seguridad adicional. Los sistemas computarizados multiusuarios necesitaron sistemas operativos que pudieran evitar interferencias intencionales o inadvertidas entre las acciones de los usuarios [3]. Las conexiones de red también acarrearon *ataques* potenciales tanto a la *seguridad física* como a la lógica. La revelación de la información no tardó en ser solo una preocupación de seguridad sino que una preocupación más generó la creación de un nuevo *servicio de seguridad*: el mantener la *integridad* de la información. El saber convencional plasmado en los libros y papers de aquella época indicaban que los gobiernos mantenían como preocupación primordial el prevenir la revelación de la información, mientras que por otra

parte, en los negocios, la preocupación primordial era proteger la *integridad* de la información. [2].

En su popular texto "Internet security and *firewalls*", Cheswick y Bellovin definen la seguridad en cómputo como "el evitar que las personas hagan cosas que no queremos que hagan a, con, en, o desde las computadoras o cualquier dispositivo periférico [5]". Si se toma esta definición, las computadoras se ven como blancos que son atacados ("...hagan a..."), o herramientas que pueden ser utilizadas ("...con, en o desde..."). Desde esta perspectiva, la seguridad en cómputo puede distinguirse claramente de la seguridad de la información. "La seguridad en cómputo no es un fin, es un medio hacia un fin: la seguridad de la información [5].".

Una definición operacional es dada por Garfinkel y Spafford en su texto "*Unix* and Internet Security": "una computadora es segura si puede confiar en que ella y su software se comportarán como usted espera" [Seguridad y comercio en el web Oreilly]. El concepto anterior es muchas veces referido como confiabilidad. Algo que hay que resaltar es que los autores intentaron que esta definición incluyera los desastres naturales y el software con errores como preocupaciones de seguridad, pero excluyeron el desarrollo del software y lo referente a la etapa de pruebas por ejemplo.

Todas las definiciones dadas hasta este momento son relativamente informales, y como resultado, no son adecuadas para desarrollar una *taxonomía* de problemas de seguridad en cómputo. Idealmente, una definición debe demarcar de manera no ambigua los límites de un campo de preocupación en seguridad en cómputo. Por ejemplo, los desastres naturales y el software con errores pueden provocar daños a los archivos, y siendo así, una (mala) definición extensiva podría referirse al daño de los archivos y estaría abarcando ambos casos muy distintos uno del otro. Comúnmente en el campo de la seguridad en cómputo no es usual considerar todos los conceptos que se encuentran involucrados de manera inclusiva. Garfinkel y Spafford incluyen estas preocupaciones en su definición de seguridad en cómputo, pero particularizan su atención en "técnicas para ayudar a mantener el sistema seguro de personas tanto internas como externas cuyos actos tienden a una destrucción y que en muchos casos tal destrucción no necesariamente es voluntaria sino que puede realizarse por ignorancia o por un mal entrenamiento". [3].

3.1.2 Definiciones de seguridad en cómputo particulares.

Hay muchos eventos que pueden provocar daños a los archivos de una computadora y se encuentran incluidos en definiciones informales de seguridad en cómputo, pero ellos están más adecuadamente referidos como parte de campos de seguridad en cómputo más particulares. El robo de un equipo de cómputo podría ciertamente provocar la pérdida de los archivos de la computadora, pero este tipo de robo es similar al robo de una máquina copiadora, un teléfono, joyería, o cualquier otro objeto físico. Los métodos para proporcionar seguridad a objetos físicos son bien conocidos y muy desarrollados y no únicamente abarcan los equipos de cómputo. Las amenazas

ambientales, tales como terremotos, inundaciones, tormentas eléctricas, fluctuaciones de energía, humedad, tormentas de arena, variación de temperatura y de fuego, pueden también provocar daños a los archivos de computadoras, pero ellos pueden causar daños a otras propiedades y en un plano secundario a los archivos de computadoras. Al parecer los autores están acostumbrados a incluir estas amenazas dentro de sus amplias definiciones de seguridad en cómputo, y con ello han excluido las discusiones o la importancia que deberían tomar de esos problemas en sus textos o papers sobre seguridad en cómputo. En este trabajo se tratará de desarrollar una definición que intente explícitamente excluir esas áreas.

Un área similar es el software. El software con errores (*bugs*) es ciertamente una amenaza a los archivos de computadoras. Un software desarrollado de manera errónea puede causar que los archivos sean dañados o perdidos. El desarrollo del software debe incluirse como un subconjunto de la seguridad en cómputo. Muchos problemas de desarrollo de software se tratan en varias materias menos en la que debería tratarse, en el campo de seguridad de software. Los errores de software claramente generan problemas de seguridad, los desarrolladores de un producto crean *vulnerabilidades* que pueden ser explotadas. En efecto, el software que es operado de manera correcta puede volverse un problema de seguridad cuando es operado de manera de la cual no fue creado. Los problemas de software se encuentran incluidos en la *taxonomía* desarrollada más adelante como una forma de expresar que las *vulnerabilidades* de un sistema pueden ser explotadas para romper la seguridad de un sistema de cómputo.

Un método común de particularizar una definición de seguridad en cómputo es concentrarse en las tres categorías de seguridad en cómputo (*servicios de seguridad*): *confidencialidad*, *integridad* y disponibilidad [4,6]. [25]

La *confidencialidad* requiere que la información sea accesible únicamente por aquellas personas que están autorizadas para ello, la *integridad* requiere que la información permanezca sin alteraciones por accidentes o por intentos maliciosos, y la disponibilidad significa que el sistema de cómputo permanezca trabajando sin degradación de accesos y proporcionar recursos a usuarios autorizados cuando ellos los necesiten. [7].

Merece especial atención la seguridad en cómputo en lo que refiere a la protección de los archivos de la computadora y en el asegurar la disponibilidad de la computadora y del sistema en red. Esta atención es demasiado importante y sirve para particularizar por lo menos dos escenarios: Primero, como se puede observar en el anexo 3-1 el tipo más común de *ataques* vistos en internet parecen ser motivados por el objetivo de ganar el acceso a una cuenta de superusuario (root) en un sistema de cómputo basado en *unix*. Más específicamente, el acceso implica utilizar el interprete de comandos o *shell* con el cual se tiene un acceso completo a los recursos de la computadora. En otras palabras el acceso buscado es hacia un proceso que tiene la atención del procesador (un

[25] *servicios de seguridad* referidos en los cuestionarios.

shell) y no necesariamente a los archivos. Muchos atacantes realmente intentan ganar acceso al proceso *shell* para posteriormente ganar acceso a los archivos.

La otra razón esta orientada en la arquitectura de seguridad de los sistemas en cómputo basados en *unix*, donde la seguridad esta basada en la protección de objetos, los cuales incluyen tanto procesos como archivos. El acceso a los procesos esta comúnmente restringido por cuentas en las que los usuarios con permisos deben realizar una sesión (login) digitando en la consola el nombre del usuario y el password asociado a éste de manera correcta. Una vez que el atacante gana el acceso a un proceso, entonces ese proceso puede ser utilizado para ganar un acceso a un archivo. En otras palabras, el accesar al sistema de archivos requiere dos pasos: accesar a un proceso, y después accesar a un archivo. Esto es ilustrado con un proceso *unix* típico, por ejemplo, la utileria /bin/cp usada para copiar archivos. Un usuario obtiene acceso a esta utileria después de que accesa correctamente en una cuenta de usuario. Accesar a la utileria /bin/cp no significa sin embargo que el usuario pueda utilizar este proceso para copiar cualquier archivo. Cuando un proceso corre, el puede accesar únicamente una colección limitada de archivos qué se encuentran asociados con la cuenta del usuario [8]. De esta manera, el usuario puede usar la utileria /bin/cp únicamente para copiar los archivos para los cuales tenga los permisos correctos para ello.

En adición al uso de procesos para accesar archivos, los procesos también pueden ser utilizados para acceder datos que se encuentran en transmisión a través de una red. Es este caso, esos datos no se encuentran contenidos en archivos que puedan localizarse en memoria primaria (la memoria volátil de acceso aleatorio de la computadora), o en una memoria secundaria (discos de almacenamiento), en vez de ello se encuentran como flujos de paquetes de datos en transmisión. Tales flujos pueden ser intervenidos por procesos en el host de origen que iniciaría la transmisión, en el host destino o en un host que se encuentre entre los dos anteriores por donde pasen los paquetes de datos.

En resumen, conceptualizando la seguridad en cómputo ha sido basada en proporcionar *confidencialidad*, *integridad* y disponibilidad en un sistema de cómputo [7] centrando la atención en los archivos que existen en un sistema.
La *confidencialidad* e *integridad* se refieren específicamente a la prevención de la revelación, alteración o eliminación de la información contenida en los archivos de computadoras [4]. Como se ha mencionado anteriormente, estos son sólo uno de los niveles de acceso en sistemas de seguridad computacional típico. Los controles de acceso son utilizados para restringir el acceso a procesos, archivos y datos en transmisión.

3.1.3 Hacia una definición más formal.

Con estas ideas en mente, ahora se utilizarán dos preguntas como punto de partida para desarrollar una definición más formal de seguridad en cómputo:

1. ¿Qué recursos son los que se intentan proteger?

2. ¿Contra qué deben ser defendidos los sistemas de cómputo?.

3.1.4 ¿Qué recursos se intentan proteger?.

Como lo sugieren las líneas anteriores, los recursos que se desearían proteger son los procesos, archivos y datos en transmisión, en computadoras y redes de computadoras como lo indica Tanenbaum.

Un proceso es básicamente un programa en ejecución. Consiste de un programa ejecutable, los datos del programa y la pila, el contador del programa, el puntero de la pila, y otros registros, y toda la información necesaria para correr el programa [8].

Un archivo es una colección de registros de datos que contiene un nombre y son considerados como una unidad por el usuario" [9]. Se encuentran generalmente almacenados en memoria secundaria (discos). Los datos en transmisión son paquetes de datos que están siendo transmitidos a través de una red.

Algunos autores sugieren incluir otros objetos, tales como bases de datos, o semáforos [8]. En el nivel de abstracción requerido para este trabajo no es necesario hacer estas distinciones. Al hacer referencia a procesos se estará asumiendo que incluyen sus variables (como semáforos) y los archivos temporales que utiliza en memoria volátil, y los archivos que utiliza de una base de datos, los directorios involucrados, etc., que se encuentran por instantes de tiempo en memoria secundaria.

Desde el punto de vista operacional, los procesos, archivos y datos en transmisión no están en categorías independientes. Mientras que los procesos pueden estudiarse de manera separada, los archivos y datos en transmisión pueden solamente alcanzarse a través de los procesos. De otra manera, antes de que un proceso sea activado este es almacenado en un archivo. El punto importante aquí es que los procesos, los archivos y los datos que son transmitidos se deben asegurar de manera separada. Esto es así porque se cree apropiado incluir las tres categorías de manera separada como "recursos que se intentan proteger".

La excepción a las líneas anteriores son los *ataques* físicos. En estos casos, los archivos o datos en transmisión pueden ser alcanzados sin accesar primero un proceso. Un ejemplo de este caso podría ser el robo de discos floppys, discos duros o computadoras completas. Como ya se ha mencionado, los métodos para proporcionar seguridad para objetos físicos es bien conocido y bien desarrollado y no únicamente aplica al equipo de cómputo. Como tal, el robo de hardware podría no estar incluido en la definición de seguridad en cómputo. Otra posibilidad podría ser el uso de extracciones de datos por cable donde se este "escuchando" el *tráfico* de la red por medio de un dispositivo externo de la red o bien vía software. Las emanaciones electromagnéticas emitidas por una computadora son llamadas "radiación Van Eck" [10] y pueden "escuchar" los datos que son procesados en una computadora.

3.1.5 ¿Contra qué deben ser defendidos los sistemas de cómputo?

Esta pregunta puede ser interpretada de varias formas. Una de ellas es como una pregunta que responda qué es lo que se esta utilizando para realizar un *ataque*. Por ejemplo, un atacante podría utilizar un código de computadora de autoreplicación, tal como un *virus* o un gusano, o bien el atacante podría correr un script *shell* que explote un *bug* de un software y vencer con ello el *control de acceso* a un proceso. Todas ellas son "herramientas" que un atacante podría usar para conseguir un objetivo (discutido más adelante). Desde el punto de vista operacional, esta interpretación es la porción "medios" de la frase "medios, maneras y fines" la cual es un paradigma común en la estrategia militar que "define objetivos, identifica cursos de acción para llevarlos a cabo, y proporcionar los recursos que soporten cada curso de acción [11]".

Otra interpretación del "contra qué defender" es la parte "fines" de la frase "medios, maneras y fines". Las computadoras deben ser protegidas contra el ultimo objetivo, el propósito, o el blanco del *ataque*. Desde este punto de vista, la seguridad en cómputo tratará de prevenir los delitos tales como robo, fraude, espionaje, extorsión, vandalismo y terrorismo.

Una tercer interpretación, también de la parte "fines" de la frase "medios, maneras y fines", ya ha sido discutida: los archivos de las computadoras y de las redes y los datos que se están transmitiendo deben protegerse de la lectura, alteración o borrado. En adición a esto, las computadoras y las redes deben encontrarse disponibles cuando se necesiten [2]. Cohen presenta este punto de vista como sigue:

Si se prescinde de las causas de protección, puede haber tres escenarios en los que las cosas podrían suceder:

1. La información libre de fallas puede comenzar a corromperse.
2. los servicios que deben permanecer disponibles pueden negarse, y/o
3. La información puede trasladarse de un lugar a otro donde no debería hacerlo. [12]

Cohen llama a cada uno de estos tres resultados como "rompimientos", los cuales llama particularmente como corrupción, negación y escape [12]. Las medidas de mitigación de los "rompimientos" ya se han discutido anteriormente, se trata de los servicios de seguridad: *integridad*, disponibilidad y *confidencialidad*.

Cada una de estas interpretaciones tiene ventajas conceptuales y limitaciones. Los procesos de las computadoras y de las redes, los archivos y los datos que son transmitidos deben ser protegidos de los medios de *ataque* tales como *virus* de computadoras, las explotaciones de las *vulnerabilidades* de los sistemas, etc. También deben de protegerse de los fines de los *ataques*: delitos, incluyendo robo, fraude, espionaje, extorsión, vandalismo y terrorismo. Los archivos y datos en transmisión deben ser

protegidos de corrupción o de escape, y las computadoras y las redes deben estar disponibles para ser utilizadas. En pocas palabras, todas estas interpretaciones que se han expresado hasta este momento sobre que proceso de computadoras y redes deben protegerse además de la conciencia de proteger a los archivos deben incluirse en la definición de seguridad en computación que se tratará de formar con este trabajo.

Ahora bien, para crear una definición comprensiva de seguridad en cómputo adoptemos nuevamente la interpretación de "medios" y "fines" presentada con anterioridad. Se ilustrará la interpretación con dos ejemplos. En el primero, un atacante copia un archivo de contraseñas (passwords) de un sistema objetivo utilizando TFTP (trivial file transfer protocol)). El programa "crack" es utilizado con el archivo de contraseñas para obtener la contraseña en claro de las cuentas de los usuarios. Una vez obtenida la contraseña el atacante utiliza telnet para obtener un acceso al sistema destino. Una vez que obtiene acceso a la cuenta del usuario, el atacante corre un script *shell* para explotar una *vulnerabilidad* y obtener los privilegios del superusuario (root) con lo que el atacante puede comenzar a copiar archivos de información sensible o de software. En el segundo ejemplo, un atacante inunda el sistema objetivo con correo electrónico de manera silenciosa, lo cual provoca que el disco duro del sistema objetivo alcance sus límites de almacenamiento y el sistema detenga su procesamiento.

Como se muestra en el primer ejemplo, los "medios" de *ataque* incluyen tftp, crack, telnet, un script *shell*, y la explotación de una vulnerabilidad del sistema operativo. Los "fines" de los *ataques* son escapes de archivos sensibles y de software. En el segundo ejemplo, los medios de *ataques* es la inundación de correo electrónico con la finalidad de negar el servicio y el sistema tendrá probabilidades altas de caerse.

Ejemplos de *ataques*	medios	maneras	fines
Copiar el archivo de passwords, ganar acceso a la cuenta dele superusuario y usar los privilegios del administrador.	tftp, crack, telnet, scripts *shell*, *vulnerabilidades* del sistema operativo.	Accesos no autorizados	Copiar archivos y software
Enviar correo electrónico hasta saturar el sistema	Programa de correo electrónico.	Usos no autorizados	Negar el servicio

En la tabla anterior se muestran las maneras empleadas en los *ataques* de ejemplo. En el primero de ellos, tftp, crack, telnet, etc. son los medios empleados para vencer los controles de acceso en el sistema para efectuar los fines de los *ataques*: copiar los archivos y el software. Aquí el atacante no tiene autorización de accesar al sistema. Este es el punto diferente del segundo *ataque* en el que el atacante tiene acceso en el sistema y tiene acceso al uso del programa de correo electrónico y en el sistema objetivo del *ataque* tiene permisos también de acceso. El acceso, sin embargo es utilizado de manera no autorizada y comienza a saturar el sistema objetivo con el envío de demasiados correos electrónicos y causa inevitablemente una caída del sistema. Esta es la naturaleza de la definición de seguridad en cómputo que indica las dos posibles "maneras" de *ataques* en computadoras y

redes, ya sea ganar accesos no autorizados o bien, teniendo un acceso autorizado se usa dicho acceso para usar el equipo de manera no autorizada.

Esta separación de "maneras" en accesos no autorizados y usos no autorizados no son mutuamente excluyentes, y el utilizar uno u otro término no son exhaustivos. De manera más específica, el acceso y el uso no se refieren al mismo concepto aunque se relacionen en un *ataque*. Por ejemplo, cuando un atacante desvía los controles de acceso (acceso no autorizado) para lograr un objetivo, el atacante también esta haciendo un uso inapropiado de las computadoras y de las redes (uso no autorizado). Una alternativa podría ser usar los dos términos: acceso no autorizado y acceso autorizado. El problema con esta combinación es el empleo de la palabra "autorizado" la cual implica no sólo el acceso sino que también la acción (uso) esté autorizado. Es más importante enfatizar en la naturaleza no autorizada de las actividades de los atacantes. Debe tenerse en cuenta que se sobreentiende que un acceso no autorizado implica que este acceso puede resultar en uso no autorizado y también en ocasiones el uso no autorizado implica accesos no autorizados.

3.1.6 Una definición formal de seguridad en cómputo.

La definición que es tratada de formularse responde en gran parte el propósito de esta investigación. Una *taxonomía* no es simplemente una estructura neutral para categorizar especimenes. Implica incorporar una teoría del universo donde los especimenes son sacados. Define qué datos serán registrados y que especimenes serán los distintivos de la categoría. Para crear la *taxonomía* de seguridad en centros de cómputo indicada un poco más adelante en este trabajo se tuvo que describir, clasificar y analizar todos los incidentes de seguridad localizados en su mayor parte en internet y que son aplicados a casi todo centro de cómputo de hoy en día. Esta es una razón primaria para ser desarrollada una *taxonomía de ataques*. También esta influenciada por las oportunidades que se han tenido viendo a atacantes que exitosamente obtienen sus objetivos en sistemas de cómputo y en centros de cómputo en general. Esta influencia, y la discusión mantenida hasta este momento permiten establecer una característica que tienen en común todos los *ataques*: un atacante intentará siempre lograr un objetivo. La definición utilizada en esta investigación es la siguiente:

La seguridad en cómputo es prevenir que los atacantes logren sus objetivos a través de accesos no autorizados o usos no autorizados de computadoras y redes.

Esta definición proporciona la demarcación deseada en el campo de la seguridad en cómputo. Concierne al daño hacia el equipo de cómputo y las amenazas ambientales quedan excluidas. El software queda incluido, pero únicamente si hay de por medio alguna *vulnerabilidad* que pueda ser explotada para proporcionar un acceso o un uso no autorizados. Tanto los medios utilizados para obtener accesos o usos no autorizados como pudieran ser *virus*, *caballos de Troya*, telnet, etc. así como los fines de los *ataques* como

corrupción, revelación, o negación del servicio ocasionando robo, espionaje, fraude, etc., son incluidos también porque todos requieren accesos no autorizados o usos no autorizados. La definición excluye los eventos no intencionales. [2].

3.2. Una *taxonomía* de *ataques* a computadoras y a redes de computadoras.

Se continúa esta platica con una breve discusión de las características deseadas en una *taxonomía*. Es seguida por una critica de *taxonomías* actuales en el campo de la seguridad en computadoras y redes. Esas *taxonomías* actuales incluyen listas de términos, listas de categorías, categorías de resultados, listas empíricas y matrices. Una *taxonomía* propuesta para los *ataques* en computadoras y redes de computadoras es presentada. Esta *taxonomía* es desarrollada de criticas hacia las *taxonomías* actuales, iniciando desde la definición de la seguridad en cómputo discutida ya, y desde un proceso o punto de vista operacional de medios, maneras y fines. Desde este punto de vista, un atacante de computadoras y/o redes de computadoras intenta alcanzar sus objetivos a través de una secuencia operacional de herramientas, accesos y resultados que unen a esos atacantes con sus objetivos. En el siguiente apartado (marco metodológico) se usará esta *taxonomía* d e *ataques* para la realización de los análisis para cada uno de los riesgos detectados.

3.2.1 Características de *taxonomías* satisfactorias.

Una *taxonomía* podría tratarse de la clasificación de categorías con las siguientes características [2].

1. Mutuamente excluyente,- La clasificación de algo en una categoría la excluye de todas las demás ya que no pueden traslaparse.
2. Exhaustiva.- Tomar a un mismo tienpo las categorías e incluir todas las posibilidades.
3. No ambigua.- De manera precisa y clara decidir en que lugar queda encasillado un término con toda certeza sin importar quien sea quien lo clasifique.
4. Repetible.- Los términos repetidos quedan encasillados en la misma clasificación sin importar quien haga la clasificación.
5. Aceptada.- Tanto lógica como intuitiva.
6. Utilizada.- Utilizada como una herramienta de ayuda en el campo de una investigación.

Estas características se pueden utilizar para evaluar las posibles *taxonomías*. Sin embargo en algunas ocasiones se tienen que flexibilizar los límites de ciertas características. Una *taxonomía* es una aproximación de la realidad que se esta utilizando en cierto momento para entender un campo de estudio. Las flexibilizaciones deben darse en el sentido en el que pueden ocurrir escenarios en los que los datos de estudio que se

desean clasificar son imprecisos o inciertos para el estudio. Sin embargo, la clasificación es un proceso importante y necesario para estudios sistemáticos.

3.2.2 Hacia una *taxonomía* de *ataques* a computadoras y redes de computadoras.

Un *ataque* es un intento de acceso no autorizado o un intento de uso no autorizado sin importar el grado de éxito. Una *taxonomía* de *ataques* por si misma tiene una gran importancia ya que facilita el desarrollo de políticas y recomendaciones para incrementar la seguridad en un centro de cómputo. Una *taxonomía* de *ataques* también puede ser usada para el desarrollo de nuevos sistemas y utilizarse en sistemas de evaluación que ya existan.

"Comparando las posibles categorías de *ataques* contra las características de un sistema objetivo, una persona podría establecer que tan seguro podría encontrarse el sistema de los *ataques* potenciales a su seguridad...." [2].

Finalmente, una *taxonomía* de *ataques* puede ser utilizada para evaluar la efectividad de los esfuerzos de mitigación de daños, tales como mayor severidad en los reglamentos y leyes, estudios, revelación de información de *vulnerabilidades*, respuestas a incidentes, etc.

En este trabajo, la *taxonomía* desarrollada se utilizará para determinar ciertas características de cada una de los riesgos existentes en las computadoras y/o en las redes de computadoras que se encuentran en un centro de cómputo.

3.2.3 *Taxonomías* actuales de seguridad en computadoras y en redes de computadoras.

Las *taxonomías* en seguridad en computadoras y redes de computadoras no necesariamente centran su atención en los *ataques* tal y como sucede en este trabajo. Por ejemplo, algunos autores dan mayor atención a la seguridad o bien a las *vulnerabilidades*, las cuales podrían ser utilizadas para llevar a cabo un *ataque*. Sin importar en que sea centrada la atención ya sea en los *ataques* o no, los autores generalmente intentan clasificar todos los *ataques*, lo cual es elemento común en las *taxonomías* como ya se ha mencionado. Para propósitos de dejar completa esta plática, se podría complementar la *taxonomía* de seguridad en computadoras y en redes de computadoras asumiendo que esa seguridad incluye *ataques*.

3.2.3.A. Listas de términos.

Una popular y simple *taxonomía* de seguridad en computadoras y redes de computadoras es una lista de términos. Ejemplos son los siguientes, para los términos digitados en mayúsculas aún no se ha encontrado un significado en español que indique lo que el autor intento expresar.

Esta es una clasificación de Cohen [12]:

caballos de Troya	TOLL FRAUD NETWORKS	gente ficticia	observación de la infraestructura	sobrecarga de correo electrónico
bombas de tiempo	Obtención de trabajos	remover los límites de protección.	interferencia a la infraestructura	ingeniería humana
sobornos	DUMPSTER DIVING	vibración favorable	adivinación de contraseñas	inserción de paquetes
DATA DIDDLING	*virus* computacionales	valores no válidos en llamadas.	errores de Van Eck	observación del contenido de paquetes
errores de PBX	SHOULDER SURFING	abrir líneas de escucha en los micrófonos.	Información de viejos discos	revisión de videos
robo de respaldos	agregación de datos	bombas de condición	Desviación de procesos	actualización de discos con datos falsos.
sobrecarga de datos de entrada	colgar anzuelos	llamadas telefónicas tramposas	Inserción de valores ilegales	EMAIL *SPOOFING*
LOGIN SOPOOFING	fallas de tensión inducida	*ataques* a los servicios de red	*Ataques* combinados	

Otra lista, ahora de Icove [13]:

conexión secreta interceptora de teléfono	DUMPSTER DIVING	EAVESDROPPING ON EMANATIONS	Negación del servicio	HARASSMENT
enmascaramiento	piratería de software	copia de datos no autorizada	Degradación de servicio	análisis de *tráfico*
Trap doors	Covert channels	*Virus* y gusanos	Session hijacking	*Ataques* de tiempo
Tunneling	*Caballos de Troya*	*IP Spoofing*	Bombas lógicas	Data diddling
Salamis	Password sniffing	Exceso de privilegios	Scanning	

He aquí una lista de términos ordenada alfabéticamente detectada por el autor en donde además de dar los términos a manera de lista se agrega una breve descripción del factor de riesgo, el *servicio de seguridad* que amenaza, el grado de prevención, detección y frecuencia.

• Analizadores de red. Puede tratarse de hardware o software o ambos.	Descripción. Lectura del *tráfico* en el medio de transmisión (medio promiscuo) que incluye cualquier texto en claro, passwords, correo electrónico y transferencia de archivos. Amenazas: *Confidencialidad.* Prevención: Imposible. Detección: Muy difícil o imposible. Frecuencia: Desconocida, pero cada vez es más común. Severidad: Potencialmente muy alta.
• Back y Trap Doors	Descripción: Un back door es alguna maldad dentro de un sistema muchas veces intencionalmente creada por el desarrollador de un sistema, en otras ocasiones creada por accidente. Un trap door es una forma de back door Errores en la codificación ya sea de manera intencional o no, que provocan un mal funcionamiento del programa o sistema liberado y por lo tanto habrá que revisar de nuevo el código o llamar al programador. Amenazas: *Confidencialidad*, aspectos legales y éticos. Prevención: Podría ser difícil. Detección: Puede ser difícil. Frecuencia: Desconocida, probablemente rara. Severidad: Potencialmente alta.
• Bombas lógicas.	Descripción. Modificación a programas de cómputo que en condiciones especiales realizan algún funcionamiento irregular. Probado en condiciones normales no revela indicios de tratarse de una bomba lógica. Las bombas lógicas pueden utilizarse para ocasionar daños/fraudes y/o pasadas, por ejemplo supóngase que se tiene el siguiente fragmento de código en funcionamiento: *if* empleado = yo *then* pago * 1.01 *else* ..... // los demás empleados. Amenazas: *Integridad*, puede afectar la accesibilidad y la *confidencialidad* Prevención: Casi imposible. Detección: Puede ser difícil. Frecuencia: Desconocida, muy rara. Severidad: Potencialmente muy alta.
• *Caballos de Troya*	Descripción. Cualquier programa que presenta un comportamiento al ejecutarse mientras realmente hace otro. Por ejemplo podríamos hablar de un protector de pantalla que mientras "salva la pantalla" destruye la *FAT* del disco duro. Los daños sufridos por *caballos de Troya* han sido: modificaciones a bases de datos, escrituras de ordenes de pago, envío de correo electrónico y destrucción de archivos y directorios (tomaron gran fuerza en los *BBS's*). Amenazas: *Confidencialidad, integridad* y accesibilidad. Prevención: Muy difícil o imposible. Detección: Puede ser muy difícil. Frecuencia: Desconocida. Severidad: Potencialmente muy alta.

• Conexiones secretas interceptoras de señales telefónicas, de microondas y satelitales. (Wiretapping).	Descripción. Incluyen intercepciones de microondas, satelitales y de radio. Amenazas: *Confidencialidad* Prevención: Muy fácil con *cifrado* de datos, de otro modo, imposible. Detección: Difícil o imposible. Frecuencia: Desconocida. Severidad: Potencialmente muy alta.
• Control de versiones.	Descripción. Debe existir un control de las versiones del software utilizado en el centro de cómputo y notificar todos los cambios realizados. Esto se hace porque la curva real del software [26] indica cómo se comporta éste a través del tiempo. El no considerar el control de versión del software produce muchas veces incompatibilidad entre los archivos y programas. No se debe pensar en resolver el problema de "versionitis" automáticamente borrando las viejas versiones de software e instalando la nueva versión. NO Remueva la versión antigua si no se esta seguro que la nueva versión pueda interpretar los archivos viejos, saber si esa nueva versión no contiene algún *bug* o si no se esta seguro que la copia es legítima. Amenazas: *Integridad* Prevención: Difícil. Detección: Difícil. Frecuencia: Común. Severidad: Potencialmente muy alta.
• Daños intencionales a datos y a programas.	Descripción. La destrucción con malicia podría ser no rastreable. Un empleado muy disgustado con la empresa, con el *site*, podría pasar un imán sobre discos flexibles dañándolos y sin dejar huella alguna. Amenazas: *Integridad* Prevención: Muy difícil. Detección: Puede ser muy difícil. Frecuencia: Desconocida, probablemente rara. Severidad: Potencialmente muy alta.
• Descuidos.	Descripción: El descuido en la operatividad de un sistema de cómputo es considerado como un "crimen computacional" por las legislaciones norteamericanas. El que un empleado con la capacitación adecuada para utilizar un sistema y un equipo de cómputo cae en un descuido y no genera las salidas esperadas puede provocar la cancelación de varios proyectos. Amenazas: Productividad. Prevención: Difícil. Detección: Puede ser difícil. Frecuencia: Desconocida. Severidad: Potencialmente alta.
• Errores de programación no intencionales.	Descripción. Los programadores generan errores cuando codifican, algunos los detectan y eliminan, otros no y permanecen en los productos como "*bugs*". Un error puede ocurrir cada 50 a 100 líneas. Un programador que genere 5,000 líneas de código por año estará generando de 50 a 100 *bugs* por año también. Amenazas: *Confidencialidad, integridad* y accesibilidad. Prevención: Imposible. Detección: Muchas veces difícil.

[26] Puede consultarse la curva real del software en el libro: Ingeniería del software de Rogger S. Pressman.

	Frecuencia: Común. Severidad: Potencialmente muy alta.
• "Escavación" de medios para obtener información.	Descripción. Se refiere a buscar todo indicio de información que ha sido desechada pero no destruida. Se puede pensar en buscar en botes de basura para buscar listas, cintas, discos flexibles, discos duros, información de tarjetas de crédito, papel carbón utilizado, etc. En otra modalidad estamos hablando de instalar software de recuperación de archivos eliminados en discos flexibles o en los discos duros. En un main frame las scratch tapes generalmente no son borradas por el usuario de mayor prioridad o por el operador del sistema y pueden contener información de interés apara realizar espionaje industrial. Amenazas: *Confidencialidad.* Prevención: Muy difícil. Detección: Muy difícil. Frecuencia: Desconocida. Severidad: Potencialmente muy alta.
• Estudio de señales electromagnéticas (emanaciones).	Descripción. Estudio de las señales electromagnéticas (conocido como ruido electromagnético) por medio de los cables que interconectan los distintos dispositivos: computadoras, impresoras, módems, monitores, teclados, conectores, amplificadores, etc. Si se cuenta con una buena antena, un escape modesto puede ser leído (los datos que se transmiten por él) a una distancia moderada. *Amenazas: Confidencialidad.* Prevención: Muy difícil. Requiere protección "TEMPEST" (estudio y control de señales electrónicas emitidas por equipos de procesamiento de datos automáticos). Detección: Imposible. Frecuencia: Desconocida. Severidad: Potencialmente muy alta.
• Fallas en el hardware.	Amenazas: *Confidencialidad, integridad* y accesibilidad. Prevención: No puede prevenirse. Detección: La mayoría de las veces fácil. Frecuencia: Común. MTBF (Mean Time Between Failure) común. Severidad: Potencialmente muy alta.
• Fingirse otra entidad (impersonation).	Descripción: Es la acción de emplear códigos de acceso para obtener permiso (acceso) de utilizar el equipo de cómputo para examinar datos, utilizar programas o simplemente usar tiempo de computadora. El empleo de dispositivos de *control de acceso* biométrico hace este tipo de actividades mucho más difíciles sin embargo no imposibles. Amenazas: *Confidencialidad, integridad,* accesibilidad. Prevención: Muy difícil. Detección: Muy difícil. Frecuencia: Desconocida. Severidad: Potencialmente muy alta.
• Fuego y desastres naturales.	Descripción: Desastres ocasionados por incendios y desastres naturales son de lo más común en los balances de pérdidas financieras de las compañías aseguradoras. Si el fuego no daña directamente al sistema de cómputo el resultado del calor, humo o agua pueden hacerlo. Si bien es cierto que ese puede preparar para una catástrofe, la preparación es incompleta si llega a ocurrir. Amenazas: *Integridad,* accesibilidad.

	Prevención: Difícil. Detección: Fácil. Frecuencia: Desconocida. Severidad: Potencialmente muy alta.
• Ineptitud (Bumbling).	Descripción: Se da cuando las personas con permiso de accesar (estar) en el centro de cómputo NO cuentan con un entrenamiento adecuado e introducen a los sistemas datos erróneos que producirán información también errónea. El término en inglés "bumbling" hace referencia a errores humanos, accidentes, errores de omisión y errores de comisión. Amenazas: *Confidencialidad, integridad* y accesibilidad. Prevención: Muy difícil. Detección: Algunas veces fácil, en otras ocasiones muy difícil. Frecuencia: Uno de los riesgos más comunes. Severidad: Potencialmente muy alta.
• Información imprecisa o caduca.	Descripción: Muchos de los riesgos referidos ignoran el tema de la calidad de la información que se esta protegiendo. De que sirve proteger a la información errónea o caduca?, éste tipo de información debe eliminarse. Por ejemplo, tener almacenada la edad de los trabajadores como caracteres planos en vez de estar almacenados como campos calculados puede provocar información imprecisa. Amenazas: *Integridad* y aspectos éticos y legales. Prevención: Puede ser muy difícil. Detección: Puede ser muy difícil. Frecuencia: Común. Severidad: Potencialmente muy alta.
• Negación del servicio.	Descripción: Es un crimen de computación relativamente nuevo. Entre las acciones que componen a este riesgo se encuentran las siguientes: • Tirar el sistema. • Bloquear los puertos. • Desconectar los periféricos. • Colocar basura en la pantalla. • Cambiar nombres de los archivos y/o directorios. • Borrar programas y/o archivos usados por otros programas o por otras personas. • Usar indiscriminadamente los recursos del sistema disminuyendo el rendimiento global del mismo y afectando con ello las actividades de las demás personas. Amenazas: Accesibilidad. Prevención: Muy difícil. Detección: Muy fácil. Frecuencia: Común últimamente. Severidad: Potencialmente muy alta.
• Perseguidor. (Piggybacking)	Descripción: Existen dos modalidades, el "perseguidor físico" y el "perseguidor lógico". Un "perseguidor" es aquella entidad que gana un acceso a donde no lo tiene después de que un usuario autorizado lo ha hecho. De ahí que un "perseguidor físico" sea aquel que obtiene un acceso al centro de cómputo o aun área que se encuentre bloqueada después de que un usuario ha digitado un password, o mostrado una identificación y ha obtenido un acceso pasando junto con la persona acreditada. Un perseguidor lógico es aquel que obtiene el acceso a un sistema después de que un usuario con permiso ha dejado de usarlo o se encuentre usándolo.

	Amenazas: *Confidencialidad, Integridad* y accesibilidad. Prevención: Muy difícil. Detección: Puede ser difícil. Frecuencia: Extremadamente común. Severidad: Potencialmente muy alta.
• Piratería.	Descripción: O piratería de software. Es el proceso de copiar software y documentación de manera ilegal y en algunos casos hasta re-empaquetándola para la venta. También en internet y en servicios de *BBS* se pueden encontrar programas listos para ser "bajados" y utilizados inmediatamente sin tener que pagar el precio de la licencia. Amenazas: Aspectos éticos y legales. Prevención: Muy difícil Detección: Puede ser difícil. Frecuencia: Extremadamente común. Severidad: Potencialmente muy alta.
• Riesgos ocupacionales por usar estaciones de trabajo, microcomputadoras y redes de computadoras.	Descripción: Existen 2 principalmente: [27] • Riesgos de radiación. • Riesgos que culminan en lesiones nerviosas por actividades exageradamente repetitivas y/o bajo mucha presión. [28] Amenazas: A la salud del usuario y su seguridad. Prevención: Puede ser difícil. Detección: Puede ser difícil. Frecuencia: Desconocida, puede ser común. Severidad: Potencialmente muy alta.
• Robo.	Descripción: Generalmente la seguridad reflejada en un centro de cómputo implica proteger el hardware, software y los archivos de destrucciones accidentales, destrucción de mala fé y de robo también de mala fé. De los 3, la destrucción accidental es la más frecuente, la destrucción de mala fé la segunda y afortunadamente el robo queda en tercer lugar, sin embargo el robo podría jamás detectarse, por ejemplo, un empleado puede fácilmente crear una copia en disco de archivos de información sensible, colocar el disco en su lugar y tranquilamente trabajar en su casa con la información hurtada. El robo puede darse en tres casos: • Robo de equipo. • Robo de información. • Robo de servicio. Amenazas: *Confidencialidad, integridad,* accesibilidad (La *integridad* no es afectada si el robo únicamente implico perder una copia de la información, como pudiera ocurrir con una cinta, un floppy, o cualquier medio de almacenamiento). Prevención: Muy difícil. Detección: Muy difícil. Frecuencia: Desconocida. Severidad: Potencialmente muy alta.
• Sabotaje.	Descripción: Es el crimen informático más común de daño físico o lógico. El daño físico ocurre cuando el perpetrador destruye el equipo de cómputo o la información, puede ser de manera violenta o incluso interrumpir momentos

[27] Consultar el American Journal of Epidemiology, Diciembre 10, 1992 San Francisco.
[28] Llamado "Repetitive Motion/Carpal Tunnel Syndrome" por los médicos de E.U.

	críticos de operaciones de escritura a un disco dañándolo. Los daños lógicos ocurren por ejemplo al cambiar las etiquetas internas o externas de los discos o al utilizar algún software para cambiar el contenido de un archivo. Amenazas: *Integridad*, accesibilidad. Prevención: Muy difícil. Detección: Puede ser fácil o muy difícil. Frecuencia: Desconocida, probablemente rara. Severidad: Potencialmente muy alta.
• Simulación y modelado.	Descripción: Utilizado generalmente para propósitos benignos pero puede ser utilizado para producir daños. Se usa la simulación y modelado para generar información con datos manipulados. Generalmente todo procedimiento es susceptible de ser modelado. Entre los casos más sorprendentes en E.U. están las modelaciones realizadas con el fin de perpetrar desfalcos económicos utilizando paquetes gráficos con los que manipularon la información para evitar detecciones en las gráficas cuando se modificaban ciertos valores. Amenazas: ? Prevención: No es posible. Detección: Varía. Frecuencia: Desconocida. Severidad: Potencialmente muy alta.
• Sobrecarga.	Descripción: La seguridad de la red está en riesgo cuando el sistema comienza a sobrecargarse. Puede terminar en un riesgo de tipo "Negación del servicio". Amenazas: Accesibilidad. Prevención: Muy difícil. Detección: Fácil. Frecuencia: Desconocida, común en sistemas que son excesivamente utilizados (donde hay demasiados usuarios). Severidad: Potencialmente muy alta.
• Tergiversación, Falsificación. (misrepresentation). (Tergiversación.- Forzar, torcer las razones o argumentos, las palabras de un texto, la interpretación de ellas, o las relaciones de los hechos y sus circunstancias).	Descripción: Uso de la computadora para engañar o intimidar para obtener un fin. Amenazas: *Confidencialidad*, aspectos legales y éticos. Prevención: Podría ser difícil. Detección: Puede ser difícil. Frecuencia: Desconocida, probablemente rara. Severidad: Potencialmente alta.
• Uso no autorizado de ciertos programas de software. (superzapping)	Descripción: SUPERZAP es una utilería disponible en sistemas de tipo mainframe para modificar, destruir, copiar, descubrir, insertar, usar o negar el acceso a datos que han sufrido algún percance. En las micros, el equivalente es "Norton Utilities" o "PC Tools". "Superzapping" es el término para hacer referencia al uso no autorizado de algunos programas (utilerías) para modificar, destruir, copiar, descubrir, insertar, usar, o negar el uso de los datos de los equipos de cómputo. El Superzapping no es detectado por ningún otro software y únicamente deja indicios en los archivos de log tanto de las main como de las micros. Amenazas: *Confidencialidad, integridad*, accesibilidad. Prevención: Muy difícil. Detección: Muy difícil. Frecuencia: Desconocida.

	Severidad: Potencialmente muy alta.
• *Virus* y gusanos computacionales.	Descripción: Programas de computadoras que se vuelven armas potenciales ya que tienen generalmente la finalidad de destruir archivos de programas o de información. Amenazas: *Integridad*, accesibilidad. Prevención: Puede ser difícil. Detección: Actualmente es relativamente sencillo. Frecuencia: 1 de cada 20 máquinas pueden estar infectadas. Severidad: Potencialmente muy alta, usualmente baja.

Las listas de términos generalmente no cumplen su propósito ya que no contienen las características de una *taxonomía* satisfactoria. En primer lugar, los términos generalmente no son mutuamente excluyentes. Por ejemplo, los términos *virus* y bomba lógica son encontrados generalmente en este tipo de listas, pero un *virus* puede contener una bomba lógica, así que las categorías se traslapan. En nuestros días los atacantes utilizan múltiples métodos en un *ataque*. Desgraciadamente en el campo del cómputo el desarrollar una lista exhaustiva podría ser muy larga y no manejable e incluso difícil de aplicar e incluso no podría indicar alguna relación entre diferentes tipos de *ataques*.

Como lo ha indicado ya Cohen, "una lista completa de cosas relacionadas a los sistemas de información es difícil crear y muy probablemente pueda estar equivocada. La gente a intentado crear listas comprensivas y en algunos casos ha producido volúmenes enciclopédicos, pero existe un número potencialmente infinito de problemas diferentes que pueden ser encontrados, así que cualquier lista que pudiese hacerse únicamente serviría para propósitos de establecer un límite [12].

Ninguna de las listas presentadas podría ser (completamente) aceptada en este trabajo. Parte de esta razón es que las definiciones mostradas en las listas no están estandarizados. Por ejemplo, cuantas veces se ha escuchado el término *virus* computacional, sin embargo no existe una definición aceptada todavía, es común encontrar cientos de definiciones a este término.

Finalmente este esquema de clasificación no proporciona una estructura para categorizar. Combinado con lo que se ha expresado en estas últimas líneas, la *taxonomía* basada en listas de términos esta limitada y por lo tanto no podría ser muy utilizada y por ende no sirve para realizar una clasificación de los *ataques* actuales en computadoras y redes de computadoras en los centros de cómputo.

3.2.3.B. Listas de categorías.

Una variante de la lista de términos es la *taxonomía* por lista de categorías. Un ejemplo de una de las listas más cuidadosamente desarrollada es dada por Cheswick y

Bellovin en su documento referente a *firewalls* [5]. Ellos clasifican a los *ataques* en las siguientes 7 categorías:

1. Robo de passwords.- Métodos utilizados para obtener las contraseñas de los usuarios de los sistemas.
2. Ingeniería social.- Hablar o expresarse de tal manera que se puede obtener información no disponible.
3. *Bugs* y backdoors.- Tomar ventaja de la implementación de los sistemas que no han sido cuidadosamente revisadas su especificaciones, o reemplazar el software con versiones comprometidas.
4. Fallas de *autenticación*.- Vencer los mecanismos utilizados para la *autenticación*.
5. Fallas de los protocolos.- Los protocolos por sí mismos no están del todo bien diseñados o implementados.
6. Fuga de información.- Uso de programas y utilerías de las implementaciones de los sistemas tales como finger o el propio DNS para obtener información que es necesaria por los administradoras para conocer el rendimiento de la red, pero que también podría ser utilizada por los atacantes.
7. Negación del servicio.- Son los esfuerzos dados para prevenir que los usuarios sean capaces de utilizar sus sistemas.

La *taxonomía* por lista de categorías es una mejora ya que proporciona una estructura, pero este tipo de *taxonomías* también sufre de algunos problemas como la *taxonomía* por lista de términos. Los autores también han intentado hacer listas basadas en estas listas así que hace que la aproximación hacia una *taxonomía* satisfactoria caiga en los inconvenientes similares a los de la *taxonomía* previa.

3.2.3.C. Categorías de resultados.

Otra variación de las *taxonomías* por métodos de listas es agrupar todos los *ataques* en categorías básicas que describen los resultados de un *ataque*. Un ejemplo es una lista tal como corrupción, fuga y negación, como es usada por Cohen [12,4] donde la corrupción se refiere a la modificación no autorizada de información, la fuga es cuando la información termina en donde no debería estar, y la negación es cuando una computadora o un servicio de red no esta disponible para su uso [12].

Rusell y Gangeemi utilizan categorías similares pero las definen utilizando términos opuestos: 1) mantener en secreto y *confidencialidad*, 2) exactitud, *integridad* y autenticidad; y 3) disponibilidad [4]. Otros autores utilizan otros términos, o usan esos términos de manera diferente.

El autor ha detectado los resultados de un *ataque* (afectaciones) manifestándose en contra de:

- La identificación de las partes que se comunican (proceso de *autenticación*) o que se identifican (identificación).
- La *confidencialidad*.
- La *integridad*.
- La disponibilidad.
  - De los recursos.
  - De la productividad.
- La salud del usuario y su *seguridad física*.
- De los aspectos éticos y legales.

Este tipo de esquema de clasificación ha proporcionado una estructura muy utilizada porque muchos *ataques* individuales pueden ser asociados únicamente con una de esas categorías. Sin embargo, este no es siempre el caso. Un ejemplo es un intruso que utiliza una computadora o un recurso de red sin degradar el servicio de los demás usuarios [2]. Este ejemplo podría no ser fácilmente asociado con una de las tres categorías típicas.

3.2.3.D. Listas empíricas.

Una variación de los resultados de la *taxonomía* de tres categorías es desarrollar una larga lista de categorías basada en una clasificación de datos empíricos. Un ejemplo desarrollado por el autor donde muestra los agentes de riesgo externos poco considerados hasta este momento pero no por ello deben dejar de considerarse es la siguiente clasificación:[29]

Riesgos por no considerar los factores externos.	A) Geológicos.	• Sismos. • Vulcanismo.
	B) Atmosféricos.	• Inundaciones. • Huracanes. • Tornados. • Tormentas eléctricas.
	C) Sociales.	• Derivadas de las concentraciones humanas. • Vandalismo. • Paros laborales, huelgas.
	D) Otros.	• Incendios. • Ruido electromagnético. • Partículas suspendidas como el humo de cigarrillos que se adhieran a la superficie de los discos de almacenamiento magnético. • Explosiones en instalaciones vecinas.

[29] Tomada del anexo III-3.

Otro ejemplo es la *taxonomía* desarrollada por Neumann y Parker para clasificar *ataques* actuales enviados al SRI Internacional como parte del "Risk Forum" ("Risks to the public in Computers and Related Systems") [14]. Neumann y Parker utilizan ocho categorías para clasificar sus datos. Una ventaja de esta aproximación es que los *ataques* que no podían lógicamente encasillar en alguna de las tres categorías tradicionales, ahora ya puede ser clasificado. La lista de Neuman y Parker es como sigue, los ejemplos son de Amoroso [2]:

1. Robo de información externa (echar un vistazo en alguna terminal).
2. Abuso de recursos (destruir una unidad de disco).
3. Disfrazamiento (grabar y reproducir nuevamente una transmisión de red).
4. Programas plaga (instalar un programa malicioso).
5. Desviando *autenticación* o autoridad (craqueo de passwords).
6. Abuso de autoridad (falsificación de registros).
7. Abuso a través de la inacción (mala administración intencional).
8. Abuso indirecto (Utilizar otros sistemas para crear un programa malicioso) [2]

Amoroso critica esta lista como sigue:

Un inconveniente de esta *taxonomía* de *ataques* podría ser que los ocho tipos de *ataques* son menos intuitivos y difíciles de recordar que los tres tipos de riesgos simples en la categorización de riesgos simples. Otra de las desventajas es que la lista de *ataques* esta basada en las ocurrencias actuales, y es difícil hacer una reestructuración para adecuar nuevos *ataques*. [2].

Los métodos de lista al parecer pueden ser convenientes utilizarlos como referencia ya que pueden clasificar un gran número de *ataques* actuales. Si fuese cuidadosamente construida una lista podría tener categorías con las primeras cuatro características deseables: mutuamente excluyentes, exhaustiva, no ambigua y repetible. Sin embargo el colocare todas las categorías de *ataques* en una única categoría no es suficiente. Como lo indica Amoroso, el resultado de generar una *taxonomía* en forma de lista podría no ser lógico e intuitivo y no proporciona una estructura adicional que muestre las relaciones entre las categorías, esto podría resultar en algo de uso limitado.

3.2.3.E. Matrices.

Perry y Wallich presentan un esquema de clasificación basado en dos dimensiones: *vulnerabilidades* y perpetradores potenciales. Esto permite realizar una categorización de incidentes en una matriz simple como la que se muestra en la siguiente figura donde las celdas individuales de la matriz representan la combinación de perpetradores potenciales: operadores, programadores, empleados de datos de entrada,

usuarios internos, usuarios externos e *intrusos*, y los efectos potenciales: destrucción física, destrucción de información, data diddling, robo de servicios, browsing, y robo de información (*vulnerabilidades*) [15,2].

	Operadores	Programadores	Entrada de datos	Internos	Externos	*Intruso*
Destrucción física	Bombing short circuits					
Destrucción de información.	Borrado de discos	Software malicioso			Software malicioso	vía módem
Data diddling		Software malicioso	Entrada de datos falsa.			
Robo de servicios		Robo como usuario		Acciones no autorizadas	vía módem	
Browsing	Robo de medios			Accesos no autorizados	vía módem	
Robo de información				Accesos no autorizados	vía módem	

Las dos dimensiones de esta matriz son una mejora sobre la dimensión sencilla de categorías de resultados que se presentó previamente. Las dos dimensiones parecen ser mutuamente excluyentes y quizá categorías exhaustivas. El uso del término *vulnerabilidad* que describe los términos de la izquierda no es generalmente aceptado, y podría ser mejor utilizar el encabezado "resultado de la explotación de la *vulnerabilidad*".

Quizá algo importante que puede destacar de esto, es que los términos dentro de la matriz no parecen ser lógicos o intuitivos. Por ejemplo, un usuario externo causa destrucción de información utilizando software malicioso. Software malicioso es un término que generalmente se asocia a un *virus* computacional o a gusanos o a *caballos de Troya*. Un usuario externo podría utilizar otra gran variedad de métodos de *ataque* para causar destrucción de información como comandos, interfaces gráficas u otras. Los otros problemas dentro de la matriz tienen problemas parecidos.

3.2.3.F. *Taxonomía* basada en procesos.

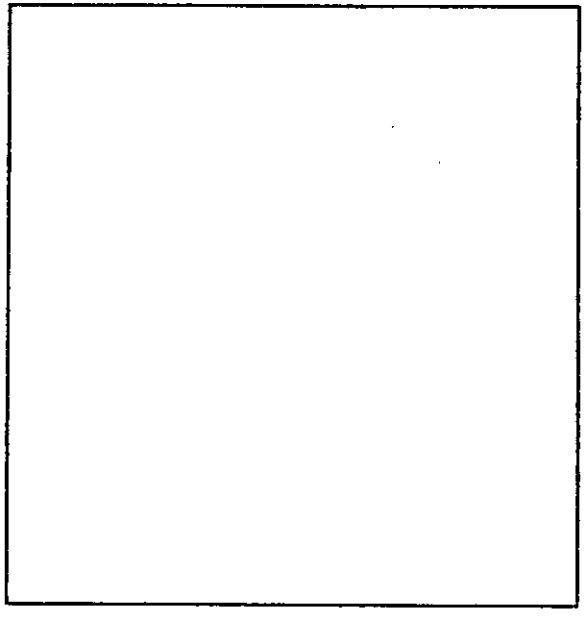
La *taxonomía* desarrollada como parte de esta investigación pareciera ser más rica que las discutidas hasta este momento ya que no intenta enumerar todas las claves de seguridad o enumerar todos los posibles métodos de *ataque*, en vez de eso intenta proporcionar una estructura muy vasta. La intención es orientar nuevamente la atención de la *taxonomía* hacia el proceso, en vez de hacerlo hacia una categoría de clasificación sencilla. Si es que se logra puede utilizarse para obtener un esquema adecuado de

clasificación de *ataques* y además una *taxonomía* que pueda ayudar en la elaboración de planes de seguridad en computadoras y redes.

Stallings presenta un modelo orientado a proceso que clasifica las amenazas de seguridad [16]. El modelo centra su atención en la información en tránsito. Stallings define cuatro categorías de *ataques* de la siguiente manera:

1. Interrupción.- Un activo del sistema es destruido o comienza a estar no disponible o comenzar en un estado de no uso.
2. Intercepción.- Una parte no autorizada obtiene acceso a un activo.
3. Modificación.- Una parte no autorizada no solo gana acceso a, sino que modifica el estado de un activo.
4. Fabricación.- Una parte no autorizada inserta objetos falsos en el sistema [16].

La intercepción es vista por Stallings como un *ataque* pasivo, y la interrupción, modificación y fabricación son vistos como *ataques* activos. Estas cuatro categorías son mostradas enseguida:



Mientras esta es una visión simplificada con utilidad limitada hace énfasis en el proceso de *ataques*. Ahora se comenzará a desarrollar un acercamiento a una *taxonomía* más comprensible que clasifica un *ataque* basado en el vasto proceso de la perspectiva operacional de "medios, maneras y fines" discutidos al inicio de este capítulo.

Desde este momento se hará referencia a un punto de vista operacional más particular.

3.2.4 Una *taxonomía* de *ataques* a computadoras y a redes de computadoras.

Desde un punto de vista operacional, un atacante de computadoras y redes de computadoras intenta alcanzar sus objetivos y/o motivaciones. El enlace es establecido a través de una secuencia operacional de "medios, maneras y fines" que unen a los atacantes con sus objetivos. Para el campo de seguridad en cómputo es apropiado usar de manera diferente y más descriptiva otros términos en vez de "medios, maneras y fines". Para esta *taxonomía*, los términos adecuados serían "herramientas, accesos y resultados". El proceso que une a los atacantes y sus objetivos en un *ataque* a computadoras y/o a redes de computadoras es mostrado en la siguiente secuencia:

Atacantes --> herramientas --> accesos --> resultados --> Objetivos

3.2.4.A. Atacantes y sus objetivos.

La gente ataca a las computadoras (y con ello a la información que contienen). Lo hacen a través de una gran variedad de métodos y son impulsados por una gran cantidad de objetivos. Como lo menciona Icove: ".... en un extremo se encuentran jóvenes "jinetes" jugando con sus computadoras y módems. En el otro extremo se encuentran los ultrapeligrosos criminales quienes intentan perpetrar en sistemas militares clasificados o en bases de datos corporativas por razones de terrorismo, o razones militares o espionaje corporativo. En la parte intermedia se encuentran los empleados molestos viendo como tomar venganza del trabajo de los demás empleados y no podían faltar aquellos antes ocultos quienes rompen los sistemas bajo contratos (*hackers*). [13].

Los atacantes son obviamente el punto de inicio, los originadores de los *ataques* en computadoras y en redes de computadoras. Generalmente el detectar a un atacante no es difícil y son públicamente conocidos, se sabe de donde son, en que salón de la escuela toman clases, en qué ciudad viven, si es un empleado de la compañía o es un extranjero, etc. etc. Son delatados básicamene por sus capacidades. Como lo indica Tiley, un atacante puede distinguirse en uno de cuatro estados: ladrones, gente meramente curiosa con competencia técnica baja, curiosos con competencia técnica alta y el *hacker* determinado con competencia técnica muy alta [17].

Rusell y Gangemi presentan dos vastas categorías de atacantes (a quienes llaman "amenazas"), los atacantes internos y los atacantes externos. Los atacantes internos incluyen a empleados, empleados anteriores, estudiantes, etc. Los atacantes externos consisten en agentes de inteligencia extranjera, terroristas, criminales, jinetes corporativos y *hackers* [4].

Cohen identifica 26 categorías de atacantes como sigue:

internos	equipos tigre	crackers ocultos	agencias de gobierno
detectives privados y reporteros	competidores	gente trastornada	guerreros de infraestructura
consultores	gente de mantenimiento	crimen organizado	rivales económicos y de la nación.
WHISTLE BLOWERS	robos profesionales	carteles de narcotráfico	organizaciones militares
hackers	HOODS	terroristas	guerreros de información
iniciados de club	vándalos	espías	
crackers	activistas	policía	

Listas similares son presentadas por Schwartau [10] y otros autores.

Una alternativa a esta estructura es identificar a los atacantes por los que ellos generalmente hacen. Icove presenta una clasificación sencilla basada en tres categorías: *hackers*, criminales y vándalos. Hace la distinción de la siguiente manera: "....son mejor diferenciados por su motivación. La motivación principal de un *hacker* es accesar al sistema o a los datos; la motivación principal de un criminal es ganar; la motivación principal de un vándalo es dañar [13]".

Los *hackers* se distinguen de los demás atacantes en que están más interesados en el reto de perpetrar la seguridad de un sistema en vez de buscar un premio financiero o de otra índole. Los jinetes corporativos y criminales profesionales por otro lado, están motivados por la victoria potencial o financiera. Los espías y terroristas buscan objetivos políticos [4]; de la misma manera los terroristas se distinguen porque buscan ganar un poder político creando miedo a través de actos provocativos. Finalmente, los vándalos son caracterizados por su enojo directo trátese así por su organización-cultura particular o simplemente por tratarse de una manera de ser.

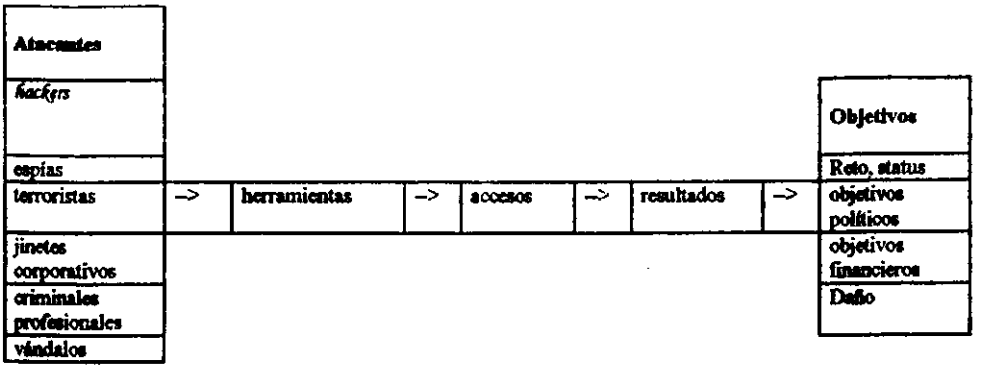
Un problema detectado por la clasificación de los atacantes en base a sus motivaciones en esas tres categorías (*hackers*, criminales y vándalos) es que, sin importar la motivación que impere, todas las categorías describen un comportamiento criminal. Como puede verse, el separar a *hackers* de vándalos no es consistente. De hecho se ha evitado esta inconsistencia no usando el término "criminal"[30] en la *taxonomía*. En vez de ello se han dividido a los atacantes en 6 categorías:

1. *Hackers*.- Rompen los sistemas de cómputo principalmente por reto personal y para dar a conocer que se pueden obtener accesos por propia cuenta.
2. Espías.- Rompen los sistemas de cómputo principalmente para obtener la información que puede ser utilizada para fines políticos.
3. Terroristas.- Rompen los sistema de cómputo principalmente para causar miedo lo cual puede servir para llevar a cabo fines políticos.

[30] Además que el término "criminal" tiene una connotación especial en México.

4. Jinetes corporativos.- Empleados de una compañía que rompen los sistemas de cómputo de sus competidores para fines financieros.
5. Criminales profesionales.- Rompen los sistemas de cómputo parafines financieros personales (no confundir con jinete corporativo).
6. Vándalos.- Rompen los sistemas de cómputo principalmente para causar daño.

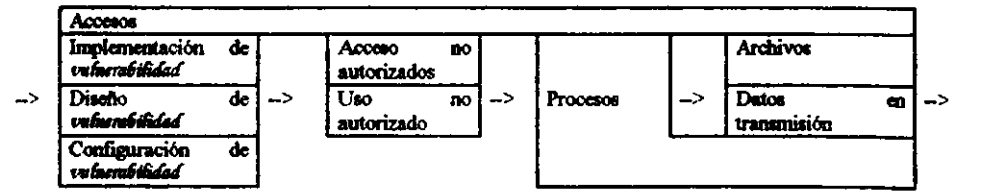
Estas seis categorías de atacantes y sus cuatro categorías de motivaciones primarias (objetivos) son mostrados en la siguiente figura:



Estas categorías de atacantes y sus objetivos que persiguen constituyen los dos extremos de la secuencia operacional de los *ataques* a computadoras y a redes de computadoras. En medio se encuentran las "herramientas, accesos y resultados" con los cuales los atacantes intentan alcanzar sus objetivos o motivaciones.

3.2.4.B. Accesos.

Antes de discutir las herramientas del proceso operacional de los *ataques* a computadoras y a redes de computadoras se abordará otro eslabón, los accesos. Si recordamos la definición de seguridad en cómputo referida al inicio de este capítulo nos trasladaremos directamente al centro de la conexión entre los atacantes y sus objetivos en esta *taxonomía*: los accesos no autorizados y/o los usos no autorizados. Enseguida se muestra el desarrollo del concepto acceso de nuestra *taxonomía*:



Las flechas muestran que todos los atacantes deben forzosamente ya sea obtener un acceso no autorizado o utilizar un sistema de una manera no autorizada, una vez que lo consigue encontrará la conexión hacia sus objetivos. Como se discutió al inicio de este capítulo el acceso o el uso no autorizado es hacia un proceso, o a los archivos y/o datos en transmisión a través de procesos.

Es importante incluir tanto a los accesos no autorizados como a los usos no autorizados en el término "maneras" de *ataque*. Los incidentes actuales de seguridad en internet (y generalmente en ambientes de redes de computadoras) involucran accesos no autorizados, sin embargo los accesos autorizados con intención de abuso son también un problema ampliamente extendido. Rusell y Gangemi estiman que el 80 % de las penetraciones a los sistemas son realizadas por usuarios autorizados con fines de llevar a cabo algún abuso computacional".

Para alcanzar el proceso deseado, un atacante debe tomar ventaja de una *vulnerabilidad* de la computadora o de la red. Tal *vulnerabilidad* es precisamente la puerta que permitirá el acceso no autorizado o el uso no autorizado [2]. Una *vulnerabilidad* puede explotarse en tres maneras. La más común y muy bien conocida es a través de un error (*bug*) del software, el cual es un problema de implementación donde el diseño es satisfactorio, pero un error fue liberado junto con la implementación tanto de software como de hardware. Existen actualmente numerosos ejemplos en los sistemas *unix* y windows NT los cuales son ampliamente difundidos en internet.

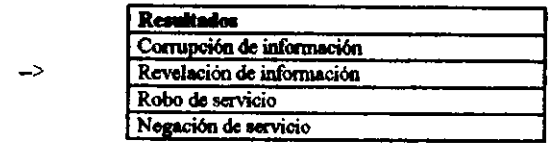
La segunda forma de una *vulnerabilidad* es la que proviene del diseño mismo la cual es potencialmente más seria y difícil de corregir. En este caso la *vulnerabilidad* es inherente en el diseño y así una implementación perfecta del diseño en el software o en hardware implica la creación de una *vulnerabilidad*. El programa sendmail de internet es un ejemplo de esto. El programa sirve muy bien y no tiene errores de software. El correo electrónico generado por sendmail puede ser utilizado de una manera no autorizada para atacar un sistema a través de un envío de correo repetitivo (mail spam) el cual causa un *ataque* del tipo negación del servicio.

La tercera forma de una *vulnerabilidad* puede provenir de un error de configuración. Estas son ocurrencias muy comunes. Muchos vendedores de software proporcionan sus productos en un estado "confiable" que es conveniente para los usuarios, pero podrían estar altamente vulnerables a sufrir un *ataque*. Los errores de configuración podrían ser tan comunes como las cuentas de los sistemas por default con passwords bien conocidos (también por default) y/o dejar los archivos bien conocidos con permisos de escritura para todo el mundo, y con ello se estarían habilitando varios servicios vulnerables.

3.2.4.C. Resultados.

El punto intermedio entre la obtención de un acceso y los objetivos de los atacantes se puede conceptualizar en los resultados de un *ataque*. En este punto dentro de la secuencia del proceso de un *ataque*, el atacante tiene acceso ya a los procesos deseados, archivos y/o datos en transmisión. El atacante ahora es libre de explotar estos accesos para alterar los archivos, negar el servicio, obtener información o utilizar los servicios disponibles. La siguiente figura representa los resultados de los *ataques* los cuales incluyen

las tres categorías tradicionales que ya se han mencionado: corrupción, fuga de información y negación, pero también se incluye una cuarta categoría: el robo de servicio [2,4,12].



Los resultados de las categorías de *ataques* se definen de la siguiente manera:

- Corrupción de información.- Cualquier alteración no autorizada de archivos almacenados en una computadora anfitrión o datos en transmisión a través de una red [2].
- Revelación de información.- La diseminación de información a cualquiera quien no este autorizado tenga acceso a ella.
- Robo de servicio.- El uso no autorizado de una computadora o de servicios de red sin degradar el servicio de otros usuarios [2]
- Negación de servicio.- La degradación intencional o bloqueo de los recursos de la computadora o de la red. [12]

3.2.4.D. Herramientas.

El eslabón final de la secuencia operacional que permite que los atacantes alcancen sus objetivos es el relativo a las herramientas de *ataque*. Se ha dejado su discusión al final ya que representa la conexión más difícil de elaborar ya que existe una amplia variedad de métodos disponibles para explotar *vulnerabilidades* en computadoras y en redes de computadoras. Cuando los autores realizan listas de métodos, ellos con frecuencia están haciendo listas de herramientas. Sin embargo, como ya se ha discutido, estas listas no pueden ser muy confiables y su utilidad es limitada, o por lo menos para esta investigación no sirven de mucho. La aproximación propuesta aquí implica las siguientes categorías:

a) **comandos de usuario**.- El atacante digita comandos en la línea de comandos o en una interface gráfica.
b) **script o programa**.- scripts y programas iniciados en la interface del usuario para explotar *vulnerabilidades*.
c) **Agente autónomo**.- El atacante inicia un programa, o un fragmento de programa el cual opera independientemente de las actividades del usuario para explotar *vulnerabilidades*.
d) **Toolkit**.- El atacante utiliza un paquete de software el cual contiene scripts, programas o agentes autónomos que explotan *vulnerabilidades*.

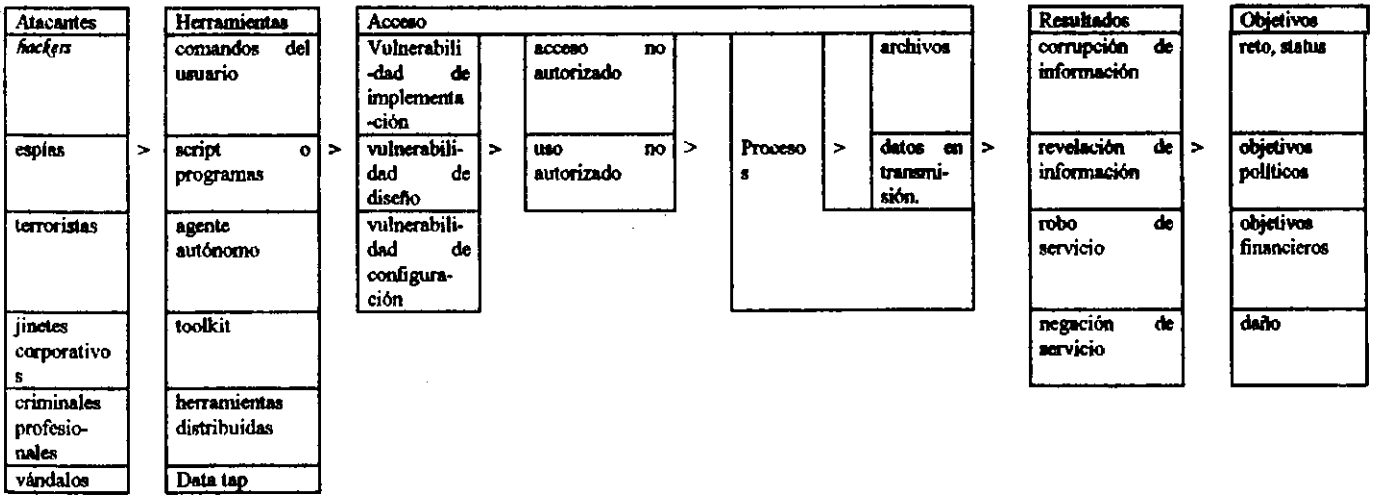
e) **Herramientas distribuidas**.- El atacante distribuye herramientas a múltiples máquinas anfitrionas, las cuales se coordinan para realizar un *ataque* en la máquina objetivo simultáneamente después de algún tiempo de espera.

f) **Data tap**.- Donde la radiación electromagnética expedida por un cable transporta *tráfico* de red, o desde una computadora anfitriona esta escuchando a un dispositivo externo a la red o a la computadora.

La siguiente figura muestra las líneas anteriores:

Herramientas
comandos del usuario
scripts o programas
agentes autónomos
toolkits
herramientas distribuidas
Data tap

3.2.5 Una *taxonomía* propuesta de *ataques* en computadora y redes de computadoras.



La figura anterior presenta la *taxonomía* completa que se ha propuesto para fines de esta investigación. La *taxonomía* representa una simplificación de la ruta que un atacante debe tomar para poder llegar a realizar sus objetivos. Para garantizar un éxito en el *ataque*, un atacante debe encontrar una o más rutas que puedan conectarse, quizá simultáneamente. Como ya lo indicaba la definición formal presentada en este capítulo, la seguridad en cómputo es prevenir que los atacantes lleven a cabo sus objetivos realizando una conexión completa a través de los pasos presentados.

En el primer bloque, atacantes, los administradores de sistemas y gente de TI deben intentar determinar quienes son y en donde se encuentran los atacantes reales y potenciales. Una vez que se ha determinado esto, los atacantes deben estar sujetos a investigación, y en caso de ser encontrados culpables de *ataques* mantener cuidado con ellos, dado que en México un *ataque* informático no es contemplado todavía como un delito entonces lo que se puede sugerir simplemente es que se traten de hacer esfuerzos para prevenir que los atacantes usen las computadoras y los recursos de red e implementar mecanismos como el cerrar cuentas de usuarios o prevenir los accesos a las conexiones de red.

Cuando las herramientas (segundo bloque del esquema) son encontradas deben ser removidas. Por ejemplo, los usuarios y administradores de sistemas son fomentados a usar software de detección de *virus* para detectar y eliminar agentes autónomos. Los sistemas se pueden monitorear de manera aislada para detectar la presencia de *caballos de Troya* o algún otro tipo de archivo colocado no autorizado. El procesamiento normal del sistema puede ser monitoreado para detectar operaciones de software no autorizado tales como "crackeadores de passwords" o "sniffers". Los comandos de usuario pueden ser monitoreados y eliminados de sesión quien este haciendo un uso indebido del sistema. El monitoreo constante puede prevenir la presencia de *ataques*, además pueden rastrearse los pasos en las actividades de los usuarios con las bitácoras del sistema. Los sistemas también pueden ser monitoreados y filtrados para el uso de forma específicas de *ataques*. Ejemplos de ello son los paquetes *IP spoofing*, mail spam y herramientas de *ataque* encontradas en toolkits comunes.

Los accesos a los sistemas pueden ser prevenidos en dos maneras. La primera de ellas es realizar un programa vigoroso para descubrir y eliminar las *vulnerabilidades* de diseño, implementación y configuración. Los administradores de sistemas son la pieza clave de este esfuerzo. Ellos deben mantener un registro y una indagación sobre todos y cada uno de los problemas que son detectados. Deben de asegurarse que el sistema y todos sus archivos estén configurados adecuadamente, todos los *bugs* del software se encuentren parchados y el software inseguro sea eliminado o restringido. El segundo método para prevenir el acceso es asegurarse que los controles de acceso en archivos y procesos estén adecuadamente establecidos e implementados. Esto incluye un amplio rango de controles, desde passwords fuertes y archivos de passwords seguros hasta corregir los permisos por default en archivos. Los accesos no autorizados pueden ser

reducidos reduciendo el número de procesos que no tengan controles de acceso y monitoreando como están siendo utilizados los procesos que se ejecutan en el sistema.

Los resultados de un *ataque* pueden ser mitigados limitando lo que un *ataque* exitoso puede acompañar. Por ejemplo, los archivos de información sensible podrían ser *cifrados*, así si un atacante exitosamente obtiene acceso a esos archivos la información podría no ser revelada (aunque esto no podría proteger nada si el objetivo del atacante es la destrucción de los archivos). Los archivos podrían también ser respaldados mitigando con ello la corrupción de información y los sistemas podrían ser cuidadosamente monitoreados para mitigar cualquier señal de un *ataque* de negación de servicio.

La técnica de mitigación podría también ser empleada en el último bloque de la *taxonomía*, los objetivos.

3.3. Conclusiones al tercer capítulo.

Una *taxonomía* no es simplemente una estructura neutral para categorizar especimenes. Implica incorporar una teoría del universo donde los especimenes son sacados. Define qué datos serán registrados y que especimenes serán los distintivos de la categoría.

Para crear la *taxonomía* de ataques a computadoras y a redes de computadoras se tuvieron que describir, clasificar y analizar a todos los incidentes de seguridad localizados en el marco teórico, además de otros que el autor ha detectado. Tales incidentes se aplican a (casi) todo centro de cómputo de hoy en día. Son tantos y tan variados los ataques a computadoras y a redes de computadoras y ni una sola clasificación inteligente que precisamente constituyen la razón primaria para desarrollar una *taxonomía* de *ataques*.

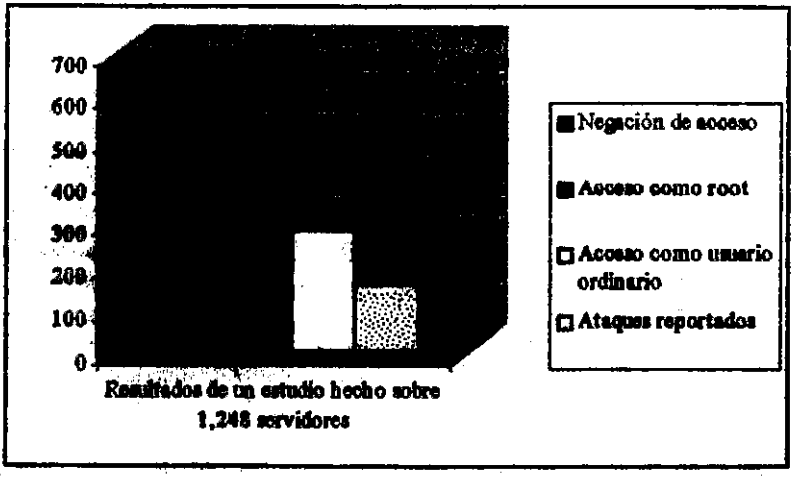
El contar con una taxonomía de ataques permitirán desarrollar un estudio referencial con un antecedente (este trabajo). Asi cada vez que ocurra un incidente podría darse una descripción detallada del tipo de incidente generado. Así sería más sencillo clasificar y darle seguimiento a los atacantes que exitosamente alcanzan sus objetivos en sistemas de computo y en centros de cómputo en general.

Una conclusión que es bueno remarcar indica que la seguridad en cómputo es prevenir que los atacantes logren sus objetivos a través de accesos no autorizados o usos no autorizados de computadoras y redes. Ahora bien, si un atacante se hace presente se puede medir con una taxonomía el nivel de ataque que intenta o intentó utilizar.

3.4 Anexos.

Anexo III-1 Tipos de ataques más comunes de internet. Estudio AFIWC.

De los 1,248 servidores atacados, 673 (54%) no permitieron el acceso. El acceso se logró con privilegios de root en 291 servidores (23%) y a nivel usuario ordinario en 284 servidores (23%). De los 1,248 ataques, 156 fueron reportados (13%) lo que significa que 1 de cada 8 ataques son reportados.



Anexo III – 2. Resumen extendido de una clasificación de seguridad en computadoras y redes de computadoras.

División de la seguridad para facilitar su estudio.	A. En los accesos (físicos y lógicos). B. Al equipo de cómputo y a otros tangibles. C. A la información en sus distintas etapas de existencia. D. Administrativa (información que no se encuentra en los sistemas de cómputo pero que esta relacionada a ellos). E. A otros

A. Seguridad en los accesos.

a) Seguridad en los accesos físicos.

Aquí se encuentran todos los controles de acceso al centro de cómputo, por ejemplo, por medio de tarjetas de identificación o el uso de sistemas de identificación de patrones.

Incluye además estudios del suministro de energía eléctrica, estudios de las condiciones del medio ambiente tales como temperatura, humedad, polvo, aire acondicionado, etc., equipo contra incendio, seguridad de los medios de almacenamiento de información.

Otros como la ubicación y construcción del centro de cómputo; riesgos de inundación; mantenimiento.

Las amenazas a la seguridad física son los desastres naturales, los accidentes y las acciones deliberadas.

b) Seguridad en los accesos lógicos.

La seguridad lógica se refiere al acceso a los sistemas de información y por ende, a la información misma.

Incluye dispositivos y acciones como asignación y cambio periódico de passwords, cifrado de archivos, restricciones de tiempo para entrar a los sistemas, log-off automático, sistemas de call-back, detección de intrusos y de intentos fallidos de ingresos al sistema.

Incluye también la asignación de permisos de acceso/manipulación de la información tales como creación, borrado, modificación, lectura, escritura, o ejecución de archivos y directorios, además la identificación de propietarios de los archivos quienes decidirán a quiénes le otorgarán las capacidades antes mencionadas.

Seguridad en los accesos (ya sean físicos o lógicos)	A) Medios de identificación (autenticación) del personal.	A1. Impersonal.	a) Uso de objetos (algo que se tiene).	• Anillo java. • Tarjetas comunes. • Tarjetas inteligentes. • Códigos de barras en dispositivos. • Uso de bandas magnéticas. • Reconocimiento de caracteres ópticos (OCR). • Reconocimiento de caracteres magnéticos (MICR).
			b) Uso de conocimientos (algo que se sabe).	• Sobrenombres. • Uso de códigos (como passwords o passphrases [31]).
		A2. Personal (algo que se es)	a) Presencial (estudio de la biometría).	• Características físicas útiles (voz, huella dáctilar, forma de la mano). • Patrón del iris. • Patrón del rostro. • Patrón de digitación del teclado.
			b) Distante.	• Firma digital.
	B) Control de acceso al edificio.	B1. Realizada por otras personas. B2. Relativo a la persona. B3. Relativo a implementaciones del propio edificio.		
	C) Control de	C1. Videocámaras. C2. Detección de		

[31] Password es una palabra empleada como contraseña. Ejemplo: cerberus123. Una passphrase es una extensión a un password. Constituye un conjunto de palabras, generalmente una frase (de ahí su nombre) utilizada como contraseña. Ejemplo: "Alicia en el país de las maravillas".

monitoreo dentro del edificio.	movimientos y/o de calor. C3. Radio frecuencia. C4. Otros.

B. Seguridad al equipo de cómputo y a otros tangibles.

- Computadoras (mainframes, estaciones de trabajo y PC's).
- Terminales.
- Equipo de comunicaciones y redes.
- Medios de almacenamiento.

C. Seguridad de la información.

La seguridad a la información se ocupa de las vulnerabilidades existentes durante la utilización de ....

- Sistemas operativos.
- Software de aplicación..
- Documentación del software (manuales y código fuente).
- Datos que están siendo procesados en cualquier tipo de computadora.
- Datos transmitidos por vía de comunicación que van desde las computadoras y hacia las mismas.
- Datos en medios transportables como discos flexibles[32] y cintas.
- Bancos y bases de datos.

Y que están presentes en distintos instantes de tiempo.

[32] Entiéndase "disco flexible" a los discos de almacenamiento secundario conocidos también como floppys.

Seguridad de la información en sus distintas etapas de existencia.	A) En la captación.	
	B) En el procesamiento.	a) Centralizado. b) Descentralizado. c) Distribuido.
	C) En la distribución o transmisión de resultados.	a) Local. c) Remota.
	D) En su almacenamiento.	a) En memoria (ROM, RAM, CACHE, etc.). b) En otros tipos de almacenamiento como cintas, discos flexibles, discos duros, etc.

Merece especial atención la etapa de transmisión de la información, actualmente la seguridad en este campo puede instrumentarse utilizando cifrado de información (de llave secreta o de llave pública o de ambas), estudiando el ruteo, usando módems o software call-back o haciendo uso de hardware y software de seguridad como firewalls, kerberos, etc.

D. Seguridad de la información en procesos administrativos.

Información que no se encuentra en los sistemas de cómputo pero que esta relacionada a ellos.

E. Seguridad a otros.

Otros tipos de seguridad que hay que considerar.	**A) Personas.**	**a) De operadores.** **b) De otras (como personal de limpieza).**
	B) Errores o mal funcionamiento de hardware.	
	C) Errores en el software.	
	D) Errores en los datos.	
	E) Daños a las instalaciones.	
	F) Rendimiento inadecuado del sistema.	
	G) Papelería como manuales de usuario y equipos.	
	H) Del ambiente que rodea al centro de cómputo.	

Merece hacer un breve comentario lo relacionado con la seguridad de las personas.

Seguridad que debe contemplarse hacia el personal del centro de cómputo.	A) Políticas de contratación. B) Procedimientos para evaluar el desempeño. C) Políticas y normatividad [33] relacionada con permisos. D) Rotación de puestos. E) Actitudes del personal.

[33] La normatividad debe contener la información de las sanciones a las cuales el o los infractores se hacen acreedores ante la primer ocurrencia así como del castigo cuando se cae en una reincidencia. No está de más

recordar que la Ley Federal del Trabajo contempla algunas instancias prohibidas a los trabajadores bajo ciertas condiciones.

Anexo III–3. Clasificación de los riesgos en ambientes computacionales.

Riesgos	1. Que amenazan la seguridad....	A. ...de la información. B. ...del equipo. C. ... de los servicios de seguridad. D. ... de la disponibilidad de los recursos. E. ... de otros (como los aspectos éticos y/o legales).	
	2. Atendiendo al lugar donde se generan pueden ser	A. Externos al centro de cómputo. B. Internos al centro de cómputo.	
	3. Cuyo origen es	A. Un factor humano.	a) Accidentales b) Deliberados. c) Por negligencia
		B. Un factor no humano.	a) Hardware b) software

2.A

Riesgos por no considerar los factores externos.

E) Geológicos.	• Sismos. • Vulcanismo.
F) Atmosféricos.	• Inundaciones. • Huracanes. • Tornados. • Tormentas eléctricas.
G) Sociales.	• Derivadas de las concentraciones humanas. • Vandalismo. • Paros laborales, huelgas.
H) Otros.	• Incendios. • Ruido electromagnético. • Partículas suspendidas como el humo de cigarrillos que se adhieren a la superficie de los discos de almacenamiento magnético. • Explosiones en instalaciones vecinas.

3.A (1/2)

Riesgos ocasionados por

A) Accidentales.	• Que tienen permiso de utilizar el equipo o de estar en el centro de cómputo.
B) Deliberados.	

personas.	C) Por negligencia.	• Que no cuentan con permiso de utilizar el equipo y/o de estar en el centro de cómputo.	**Hackers. Crackers. Phrakers.**

3.A (2/2)

Riesgos derivados de no contar con seguridad en el personal que labora en el centro de cómputo.	Ocasionan "crímenes informáticos" [34] tanto individuales como colectivos tales como:	• Espionaje industrial. • Fraude. • Desfalco-peculado. • Falsificaciones. • Robo de información. • Empleados vendiendo información. • Actos de venganza. • Bombas. • Destrucción intencional.

3.B

Riesgos en las comunicaciones:	A) Pasivos.	• Que atacan la confidencialidad. También es llamado "intercepción". Puede servir como base para ataques activos y para análisis de tráfico.[35]
	B) Activos.	• Que atacan la disponibilidad (dañando el canal). Daño en medios físicos o un daño en la infraestructura de la empresa de servicios portadores. • Que atacan la integridad de la información modificándola. • Que atacan la autenticidad (hacerse pasar por un cliente o por un host).

3.B.b.

Riesgos ocasionados por gusanos y virus.	A) Causando males no destructivos.	
	B) Causando males destructivos (como el gusano Internet o el virus NATAS).[36]	• Daños corregibles. • Daños no corregibles.

[34] El término "crimen informático" (aún) no se encuentra contemplado en las leyes mexicanas.

[35] En la feria anual de computadoras CeBIT que se celebra en Alemania, se vendió por 80 dólares un scanner con el que se puede escuchar cualquier llamada telefónica analógica inalámbrica que se haga en una distancia corta. Fuente: Periódico Humanidades No. 167 página 29 artículo "La tecnología y el robo de datos".

[36] En ambos casos, trátese de males no destructivos o de males no destructivos los virus afectan: a) los programas de propósito general, b) Los archivos del sistema operativo, c) el sector de inicio del disco, o d) la FAT.

IV. MARCO METODOLÓGICO.

4.1. Variables.

Después de haber recabado la información suficiente en el marco teórico sobre el tema de desarrollo y además de haber propuesto en el marco conceptual toda una *taxonomía* comprensiva para la clasificación de *ataques* e incidentes de seguridad en computadoras y redes; tanto la variable independiente como las variables dependientes declaradas en el marco problemático permanecen sin cambio alguno. A continuación se reproducen:

4.1.A. Variable independiente.

Presentación del problema en su causa:

Si un centro de cómputo realiza un análisis de los riesgos que afectan a la información que captan, procesan, despliegan, distribuyen y/o almacenan.

La presentación del problema en su causa permanece sin cambios con el estudio llevado a cabo hasta el momento.

4.1.B. Variables Dependientes

Presentación del problema en sus efectos:

se puede crear un plan de reducción de riesgos con objetividad.
se pueden determinar algunas necesidades no detectadas en la empresa.
se pueden cuantificar los riesgos a los cuales están sujetos los activos.
se puede estimar la probabilidad de ocurrencia de cada riesgo latente.
se pueden revisar y redefinir los controles de seguridad ya existentes.
se pueden asignar para su estudio pocos recursos tanto humanos, financieros y/o materiales.
se pueden conocer los *servicios de seguridad* con que cuentan los procesos que la utilicen (a la información).
se pueden establecer bases para una toma de decisiones.

La presentación del problema en sus efectos permanece sin cambios con el estudio llevado a cabo hasta el momento.

4.2 Variables de control.

Intervinientes.
Distorcionantes.

4.3 Hipótesis definitiva.

Después de haber recabado la información necesaria en el marco teórico sobre el tema desarrollado y además de haber propuesto toda una *taxonomía* comprensiva para la clasificación de *ataques* e incidentes de seguridad en computadoras y redes, la hipótesis declarada en el marco problemático queda sin cambio alguno.

Enseguida se reproduce:

"Si un centro de cómputo realiza análisis de los riesgos que afectan a la información que captan, procesan, despliegan, distribuyen y/o almacenan entonces se pueden crear planes de reducción de riesgos objetivos, se pueden determinar algunas necesidades no detectadas en la empresa, se pueden cuantificar los riegos a los cuales están sujetos los activos, se puede estimar la probabilidad de ocurrencia de cada riesgo latente, se pueden revisar y redefinir los controles de seguridad ya existentes, se pueden asignar para su estudio pocos recursos tanto humanos, financieros y/o materiales, se pueden conocer los servicios de seguridad con que cuentan los procesos que la utilicen (a la información) y se pueden establecer bases para una toma de decisiones".

4.4 Definición del universo.

El universo se define como el conjunto de todas las mediciones de interés del investigador. [57]

Dada la naturaleza de esta investigación, el universo de estudio puede generalizarse y hacer participe a todo encargado de seguridad, o en su defecto, de auditoria en centros de cómputo donde, tal y como lo indica la hipótesis definitiva de trabajo, se capte, procese, despliegue, distribuya y/o almacene información, no importando si tal centro de cómputo cuente o no con ambiente de redes de computadoras.

Lo que es cierto es que en todo centro de cómputo se encontrarán latentes un sinnúmero de agentes potenciales de riesgo que en cualquier momento podrían manifestarse y hacerse presentes.

---

[57] Estadística para administración y economía.
William Mendenhall y James Reinmuth
Grupo Editorial Iberoamérica.
Traducido por el maestro Joaquín Díaz Saiz del I.I.M.A.S. U.N.A.M.
México 1981
ISBN 968-7270-13-6

4.5 Determinación de la muestra.

En estudios como éste no se intenta realizar una prueba plena y mucho menos convencer a ninguna persona de que la presentación del problema en sus efectos son factores suficientes para someter a investigación la hipótesis de trabajo.

En la mayoría de los casos es impracticable o imposible observar a todos los elementos que componen el universo, por lo que se debe seleccionar una muestra de la población. Tal población se menciona en el apartado denominado "definición del universo" en este mismo capítulo.

A un subconjunto de observaciones seleccionado a partir de una población se le denomina muestra. [38] En este estudio la muestra se ha conformado por opiniones calificadas, en algunos casos opiniones de representantes directivos de TI que el autor ha considerado como criterios aceptables y que además por razones de facilidad en la aplicación, apoyan la hipótesis de trabajo como válida.

El interés por la muestra se basa en la probabilidad de describir con ella a la población de la cual fue extraída.

La unidad muestral [39] que en este estudio se llevará a cabo será de juicio. El muestreo de juicio es una de las formas de muestreo no probabilístico. La muestra se compondrá de organizaciones de diversa índole.

La finalidad es comprobar si en las empresas que constituyen la muestra cuentan o no cuentan con un estudio serio sobre riesgos en computadoras y en redes de computadoras.

La muestra se compone de las siguientes organizaciones (citadas en orden alfabético):

Centro de Cómputo de la Facultad de Ingeniería.
Consultoría de Sistemas e-commerce S.A. de C.V.
Dirección de Cómputo para la Administración Académica.
Grupo Financiero Bancomer.
Grupo Nacional Provincial.
Hussmann American.
IBM México.

---

[38] Probabilidad y estadística para ingeniería y administración.
William W. Hines y Douglas C. Montgomery
Compañía Editorial Continental S.A. (CECSA)
Segunda impresión mayo de 1987
ISBN 0-471-04759-7
México.

[39] Unidad muestral.- Colección disjunta de elementos de la población.

InfoSyst S.A. de C.V. Miembro Fundador de AMITI (Asociación Mexicana de la Industria de Tecnologías de Información). Miembro de la Asociación Mexicana para la Calidad de Ingeniería de Software (AMCIS).
Secretaría de Hacienda y Crédito público. TESOFE.

4.6 Definición del método de la investigación.

Los usuarios que integran la muestra utilizan la tecnología de información orientada a la seguridad ya sea de manera cotidiana o por lo menos en las decisiones directivas de compra/adquisición, por ende se infiere que la mejor forma de comprobar la eficiencia de las conclusiones derivadas de este trabajo es recabando la opinión de cada uno de los miembros que componen la muestra determinada antes, para ello se ha elegido como método de investigación empleado más adecuado la combinación entrevista-cuestionario-observación, el cual esta conformado en su gran mayoría, por preguntas no tan abiertas para facilitar la interpretación de los resultados obtenidos.

4.7. Costo (estimado) de la investigación.

Tiempo estimado de realización de la investigación: 10 meses, abarcando actividades de:
Diseño y recopilación de información.
Muestreo.
Ajustes
Trabajo de fondo.

Los costos de la investigación se incurren en los siguientes rubros:

Sueldo de personas.
Rentas.
Mobiliario y equipo.
Papelería y artículos diversos de oficina.
Gastos diversos.
Teléfonos.
Internet.
Correo.
Transportación.
Viáticos.

Sueldos de personas.

Persona involucrada: 1 Investigador.
Sueldo mensual: $ 14,000.00
Horas dedicadas al día: 6 horas.
Días considerados por mes: 30.5
Parte proporcional al mes por el tiempo laborado: $ 10,500.00
Costo por aplicar por los diez meses..... $ 105,000.00

Rentas.

1 estación de trabajo
SPARC 5
Renta por hora = $ 12.00
Uso de la estación por mes = 40 horas.
Costo a aplicar por mes = $ 480.00
Costo a aplicar en todo el procedimiento ..... $ 4,800.00

Mobiliario y equipo.

2 escritorios.
Valor de escritorio 1= $ 1,200.00
Vida útil = 10 años.
Factor de depreciación = (1/120)
Criterio de valuación = Valor de reposición.
Depreciación mensual = 10
Porcentaje de uso en el procedimiento = 60 %
Costo a aplicar por mes = $ 6.00
Costo a aplicar en todo el procedimiento ..... $ 60.00

Valor de escritorio 2 = $ 750.00
Vida útil = 10 años.
Factor de depreciación = (1/120)
Criterio de valuación = Valor de reposición.
Depreciación mensual = 6.25
Porcentaje de uso en el procedimiento = 50 %
Costo a aplicar por mes = $ 3,125.00
Costo a aplicar en todo el procedimiento..... $ 31,250.00

2 sillas

Valor de silla 1 = $ 500.00
Vida útil = 10 años.
Factor de depreciación = (1/120)
Criterio de valuación = Valor de reposición.

Depreciación mensual = $ 4.16
Porcentaje de uso en el procedimiento = 60 %
Costo a aplicar por mes = $ 2.49
Costo a aplicar en todo el procedimiento ..... $ 24.90

Valor de silla 1 = $ 350.00
Vida útil = 10 años.
Factor de depreciación = (1/120)
Criterio de valuación = Valor de reposición.
Depreciación mensual = $ 2.91
Porcentaje de uso en el procedimiento = 50 %
Costo a aplicar por mes = $ 1.45
Costo a aplicar en todo el procedimiento ..... $ 14.50

1 PC
Valor de computadora PC Pentium III = $ 11,500.00
Vida útil = 4 años.
Factor de depreciación = (1/48)
Criterio de valuación = Valor de reposición.
Depreciación mensual = $ 239.58
Porcentaje de uso en el procedimiento = 85 %
Costo a aplicar por mes = $ 203.64
Costo a aplicar en todo el procedimiento ..... $ 2,036.40

1 impresora
Valor de Impresora HP Deskjet 420 = $ 850
Vida útil = 4 años.
Factor de depreciación = (1/48)
Criterio de valuación = Valor de reposición.
Depreciación mensual = $ 17.70
Porcentaje de uso en el procedimiento = 10 %
Costo a aplicar por mes = $ 1.77
Costo a aplicar en todo el procedimiento ..... $ 17.70

Papelería y artículos diversos de oficina.

1 millar de hojas.
Papel bond.
Valor por millar = $ 88.00
Hojas utilizadas = 1300 aproximadamente.
Criterio de valuación = Valor de reposición.
Costo a aplicar ..... $ 114.40

Papelería en general.

(boligrafos, lápices, correctores, clips, etc.)
Criterio de valuación = Valor de reposición.
Costo a aplicar en el procedimiento..... $ 500.00

Elementos de estudio.

Libros ..... $ 1,260.00

Gastos diversos.

Teléfono

Porcentaje de aplicación = 8 %
Porcentaje de utilización en el procedimiento = 30 %
Pago mensual = $ 530.00
Costo a aplicar por mes = $ 12.72
Criterio de valuación = consolidación.
Costo a aplicar en el procedimiento ..... $ 127.20

Internet

Porcentaje de aplicación = 60 %
Porcentaje de utilización en el procedimiento = 70 %
Pago mensual = $ 320.00
Costo a aplicar por mes = $ 134.40
Criterio de valuación = consolidación.
Costo a aplicar en el procedimiento ..... $ 1,344.00

Correo electrónico.

Porcentaje de aplicación = 6 %
Porcentaje de utilización en el procedimiento = 5 %
Pago mensual = $ 320.00
Costo a aplicar por mes = $ 0.96
Criterio de valuación = consolidación.
Costo a aplicar en el procedimiento ..... $ 9.60

Transportación

Porcentaje de aplicación = 10 %
Porcentaje de utilización en el procedimiento = 10 %

Pago aproximado por viaje dentro del D.F. del centro de estudio al centro más lejano (enep aragón) = 15 pesos.
Otros viajes (dentro de *ciudad universitaria*), $3.00 por viaje, aproximadamente 120.
Costo a aplicar por mes = $ 36
Criterio de valuación = consolidación.
Costo a aplicar en el procedimiento ..... $ 375.00

Cédula resumen de costos en la investigación:

Recursos humanos	$ 105,000.00
Rentas	4,800.00
Mobiliario y equipo	33,403.50
Papelería y artículos diversos de oficina	614.40
Elementos de estudio	1260.00
Gastos diversos	1,855.80
Total a aplicar en el procedimiento	$ 146,933.70

4.8 Colaboradores y apoyos.

Afortunadamente comienza a generarse en México la curiosidad por este tipo de estudios, sin embargo en muchos aspectos aún se encuentra el cómputo en nuestro país un tanto rezagados.

Un apoyo siempre presente se dió por parte de la L.I. Nora E. Tapia Ruiz Jefe del Departamento de Control de Calidad y Auditoria Informática se la Subdirección de Sistemas de la D.G.S.C.A. e-mail: nora@dgsca.unam.mx.

El único centro de investigación en donde se ha encontrado una verdadera apertura y disponibilidad en todo momento ya sea de manera presencial o bien vía servicio de internet es el Área de Seguridad en Cómputo (ASC) de la D.G.S.C.A.

Actualmente el equipo de trabajo se encuentra enriqueciendo un sitio web localizado en: http://www.asc.unam.mx/Informacion/informacion.html [40]. En este sitio se pueden encontrar enlaces a páginas con información generada por el propio equipo del ASC o bien a manera de compendio o referencia de los mejores materiales actualizados en materia de seguridad.

Se pueden encontrar los siguientes enlaces:
Conceptos básicos de seguridad.

[40] Enlace visitado el día 8 de julio del 2000.

Tutoriales.
Bibliografía.
Otros sitios de seguridad.
Otras organizaciones de seguridad.
Las preguntas más frecuentes de seguridad en cómputo.
Proveedores de equipo.
USENETS de seguridad.

De manera personal también es bien recibida aquella persona interesada en el tema.
El personal del área de seguridad en cómputo esta compuesto por:
Juan Carlos Guel López. Jefe a cargo. Email: cguel@asc.unam.mx
El personal de investigación esta formado por:
Rodrigo López Valencia. Email: lopez@asc.unam.mx
Alejandro Núñez Sandoval. Email: nusa@asc.unam.mx
Rubén Aquino Luna. Email: ruben@asc.unam.mx

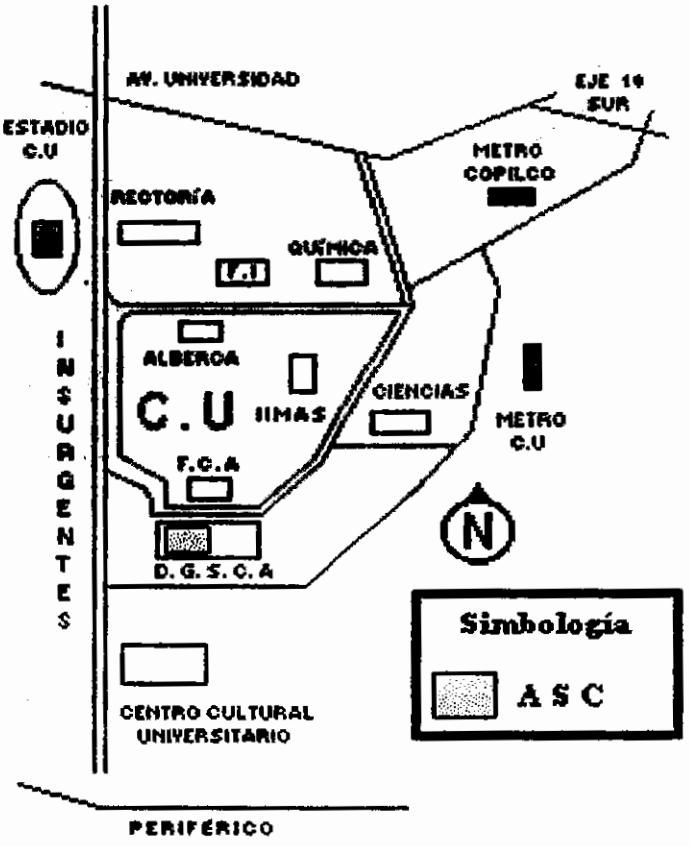
Colaboradores del ASC:
Diego Zamboni. WebSite: http://www.cs.purdue.edu/people/zamboni
Ernesto Ordoñez Cabezas.
Israel Quiroz Plata
Cesar Vega Calderón
Gunnar Wolf [41]

[41] Contribuyó también en el marco problemático de este trabajo de investigación.

El ASC ofrece una gran cantidad de medios para comunicarse con la comunidad de cómputo cuando así se requiera, los cuales se dan a continuación:
Correo electrónico: asc@asc.unam.mx
Teléfono: 5622-81-69
Fax: 622-80-43
URL: http://www.asc.unam.mx

Dirección: Dirección General de Servicios de Cómputo Académico Circuito Exterior, C. U. (frente a la FCA)
04510 México D. F.

Ubicación:



4.9 Construcción del cuestionario (cuestionario piloto).

El siguiente cuestionario se elaboró como parte de la investigación y el mismo se aplicó a cada uno de los representantes del área de seguridad y/o auditoria en centros de cómputo que resultaron ser elementos de la muestra.

El cuestionario toca los puntos esenciales y relativos a la problemática ya tratada en las variables establecidas, y que fueron mencionadas anteriormente.

Enseguida se muestra el diseño de las preguntas que componen el cuestionario aplicado además de su justificación y la respuesta esperada en cada caso.

Una copia del cuestionario que se ha aplicado se encuentra en el anexo IV-1.

Pregunta No. 1
¿Cuenta su centro de cómputo con un plan de reducción de riesgos hecho con objetividad?
Justificación: Esta pregunta permite percibir de primer instancia el valioso sentido de las preguntas y respuestas posteriores. El cuestionado podría contestar afirmativamente en cuyo caso las demás preguntas tendrían un sentido valioso. En caso de contestar negativamente entonces quizá las demás preguntas y respuestas muestren una falta de interés en el campo de la seguridad en la organización objetivo.
Respuesta esperada: sí.

Pregunta No. 2
¿Qué necesidades se han detectado en la organización derivadas de realizar estudios de *análisis de riesgos* y/o de seguridad?
Justificación: El realizar un *análisis de riesgos* es el producto derivado de un proceso de conciencia organizacional. El que una empresa se haya decidido por realizar uno de ellos es porque detecto determinados factores de riesgo que en cualquier momento podrían manifestarse. Sin embargo, una vez realizado un *análisis de riesgos* los beneficios generados pueden ser tantos como visión se tenga, pueden ir desde detectar un "ok, definitivamente se necesitan antivirus en las PC's", hasta "ok, definitivamente es necesario realizar planes de contingencia general en todo el centro de cómputo".
Respuesta esperada: varía.

Pregunta No. 3
¿Cómo se cuantifican los riesgos a los cuales están sujetos los activos cuando se realiza un *análisis de riesgos* o un estudio de seguridad?
Justificación: Permite conocer el punto de vista de los encargados de la seguridad sobre el tipo de cuantificación contemplada en los activos.
Respuesta esperada: varía aunque se piensa predomine la cuantificación monetaria.

Pregunta No. 4

¿Cómo se estima la probabilidad de ocurrencia de cada riesgo después de haber realizado un *análisis de riesgos* o un estudio de seguridad?
Justificación: Las respuestas derivadas de esta pregunta reflejan el interés posterior a un *análisis de riesgos*. El pintar una pared después de que las inclemencias climáticas la han arruinado no es una solución tajante al problema, habrá que pensar en instalar canaletas, impermeabilizantes, reforzamiento de paredes, etc.
Respuesta esperada: varía.

Pregunta No. 5
¿Cómo permanecen los controles de seguridad ya existentes después de realizar un *análisis de riesgos* o un estudio de seguridad?, ¿inalterables?, ¿sí son modificados?
Justificación: Esta pregunta permitirá saber si un *análisis de riesgos* permite rediseñar los controles existentes y con ello crear ahora controles preventivos y quizá controles correctivos para las posteriores manifestaciones de factores de riesgos.
Respuesta esperada: varía.

Pregunta No. 6
¿La asignación de recursos humanos, financieros y/o materiales se ve modificada cuando se realiza un *análisis de riesgos* o un estudio de seguridad?
Justificación: Se esperaría que lo más prudente después de llevar a cabo un *análisis de riesgos* en computadoras y redes de computadoras es encauzar los recursos indispensables, ni en mayor ni en menor número, para el buen funcionamiento de todos los procedimientos involucrados en las actividades generadas en el centro de cómputo.
Respuesta esperada: sí, después de realizar un *análisis de riesgos* se modifica la asignación de los recursos humanos, financieros y/o materiales.

Pregunta No. 7
Cuando se realiza un *análisis de riesgos* y/o un estudio de seguridad en el centro de cómputo, ¿se pueden detectar los *servicios de seguridad* que tienen los procesos que utilizan la información?
Justificación: Esta pregunta permitirá conocer si derivado de un análisis objetivo de los riesgos que afectan a la información se pueden detectar los servicios de *autenticación, control de acceso, confidencialidad, integridad*, disponibilidad y *no repudio* de los datos que son utilizados en los distintos procesos que se llevan a cabo en un centro de cómputo.
Respuesta esperada: sí.

Pregunta No. 8
¿El realizar un *análisis de riesgos* permite establecer las bases para una correcta toma de decisiones en materia de seguridad en su organización?
Justificación: En esta pregunta se puede detectar si un estudio de riesgos va más allá de un simple registro de amenazas y se considera como un instrumento de suma importancia para los encargados de la TI.
Respuesta esperada: sí.

4.9.1 Aplicación del cuestionario piloto.

La finalidad de aplicar un cuestionario piloto, previo a la aplicación formal del cuestionario final es detectar que las preguntas formuladas estén redactadas de tal manera que sean completamente entendibles, precisas, que no se presten a más de una interpretación, que estén bien redactadas y que sean lo suficientemente extensas como para que sus respuestas nos permitan aprobar o desechar la hipótesis definitiva de trabajo.

Se aplicaron cuatro entrevistas y de la misma manera se permitió observar las condiciones generales con las que cuentan las instalaciones computacionales de los encuestados. Ellos fueron:

Rodolfo Reynoso B.
RRB
Empresa Integradores de Tecnología
Depto. Administración de IT

Víctor Figueroa Peña.
VFP
TESOFE
Depto. Administración de sistemas y desarrollo.

Lic. Luis Martínez G.
LMG
Banamex.
Depto. División Productos de financiamiento Inmobiliario

Lic. Carlos Rey T.
CRT
Meta Data
Depto. Soporte técnico y puesta a punto.

A continuación se resumen y analizan las respuestas proporcionadas por las personas encuestadas:

1. ¿Cuenta su centro de cómputo con un plan de reducción de riesgos hecho con objetividad?			
	Si	No	Otra respuesta.
RRB		*	
VFP			En parte.
LMG	Si. Entendiendo por objetividad el planteamiento de las eventualidades lógicas que puedan presentarse en cualquier momento las cuales permitan detallar un plan de contingencia que se implemente conforme a los objetivos primordiales que permitan el aseguramiento de la información.		
CRT		*	

2. ¿Qué necesidades se han detectado en la organización derivadas de realizar estudios de *análisis de riesgos* y/o de seguridad?	
RRB	Tener un esquema de seguridad.
VFP	Solo se contemplan riesgos evidentes, considero que las áreas dedicadas a la seguridad informática no están tan involucradas en el desarrollo como para poder completar estudios fieles.[42]
LMG	Con la organización directamente se han tenido que desarrollar unidades o grupos específicos de trabajo que evalúan constantemente los riesgos inherentes para la seguridad informática. De igual forma se han implementado otros grupos de trabajo de *análisis de riesgos* que permiten detectar con oportunidad los posibles eventos que puedan impactar en la operación de los sistemas permitiendo resguardar de manera anticipada la información y no recurrir a planes correctivos, si no preventivos.
CRT	Sólo se ha configurado el *firewall* para que no se pueda accesar a los servidores de correo electrónico de la empresa desde nodos externos, es decir, desde casa.

3. ¿Cómo se cuantifican los riesgos a los cuales están sujetos los activos cuando se realiza un *análisis de riesgos* o un estudio de seguridad?	
RRB	Se cuantifican mediante un seguro del equipo mas no de la información. A la fecha no se ha realizado ningún estudio a detalle.
VFP	Considero que no están cuantificados, solo se detectan los más evidentes y se hacen "estrategias" sin objetivos, ni la aplicación de soluciones. Evidentemente por la falta de contacto con el área de desarrollo.

[42] Quizá aquí valga hacer mención que respuestas como ésta dejan apreciar completamente la panorámica que circunda el ambiente de cómputo del encuestado. Decir que sólo se contemplan riesgos evidentes pareciera que es muy irresponsable por parte de los encargados de la administración de la T.I.

LMG	La cuantificación de riesgos se efectúa a través de un modelo de parametrización riesgo/evento/activo, el cual determina de manera cuantitativa el efecto negativo que una situación de riesgo puede afectar no solo al área de Seguridad Informática, sino además a toda la organización y a los propios usuarios de la información. Existe un modelo matemático que permite obtener en cifras el impacto esperado en caso de una eventualidad que ponga en riesgo los recursos informáticos así como la misma información.
CRT	No se han cuantificado los riesgos de los activos en la empresa.

4. ¿ Cómo se estima la probabilidad de ocurrencia de cada riesgo después de haber realizado un *análisis de riesgos* o un estudio de seguridad?	
RRB	La probabilidad nosotros siempre la tenemos latente; de ahí que tengamos servidores de respaldo y hacemos respaldo de información del diario.
VFP	No esta estimado o no se ha difundido lo necesario.[43]
LMG	Con base en los resultados que arroje el propio análisis, de otra forma seria una estimación subjetiva sin validez.
CRT	No se han establecido las probabilidades de ocurrencia de riesgos de los activos en la empresa.

5. ¿Cómo permanecen los controles de seguridad ya existentes después de realizar un *análisis de riesgos* o un estudio de seguridad?, ¿inalterables?, ¿si son modificados?

	inalterados	Modificados	Otra respuesta.
RRB			Me imagino que deben ser modificables ya que siempre hay riesgos que nunca tomas en cuenta y salen hasta que haces un estudio detallado.
VFP			Lo ignoro.
LMG		De igual forma se evalúan con base en el estudio realizado y de ser necesario se modifican. Esto ocurre la mayoría de las veces ya que por lo general los planes de contingencia deben de ser actualizados constantemente.	
CRT			Pues como nunca se han hecho ....

6. ¿La asignación de recursos humanos, financieros y/o materiales se ve modificada cuando se realiza un *análisis de riesgos* o un estudio de seguridad?

	Sí	No	Otra respuesta.
RRB	SI porque tal vez tengas que comprar software o hardware e instalarlo ya que todo		

[43] Comprueba la última nota a pie de página.

	tiene un costo.		
VFP			Lo ignoro.
LMG			Sólo cuando es realmente necesario con base en los resultados. Sin embargo el recurso que más se afecta es el financiero y material, ya que el recurso humano no es constantemente modificado, es decir, no existe un alto índice de rotación de personal por la misma seguridad informática.
CRT			Sin comentarios.

7. Cuando se realiza un *análisis de riesgos* y/o un estudio de seguridad en el centro de cómputo, ¿se pueden detectar los *servicios de seguridad* que tienen los procesos que utilizan la información?			
	Sí	No	Otra respuesta.
RRB			Como tal nunca lo hemos hecho pero al menos procuramos tener a salvo la información que es lo que cuesta más.
VFP			Creo que no existen.
LMG	Sí, ya que es una parte esencial en el estudio a realizar, de hecho deben de ser analizados a detalle para validar su confiabilidad y vigencia.		
CRT			Sin comentarios

8. ¿El realizar un *análisis de riesgos* permite establecer las bases para una correcta toma de decisiones en materia de seguridad en su organización?			
	Sí	No	Otra respuesta.
RRB			
VFP	Por supuesto, siempre y cuando se hagan, o al hacerlos se de difusión y las políticas embonen con la forma de trabajo de toda el área de sistemas, el *análisis de riesgos* permite obtener un traje a la medida en los sistemas siempre y cuando sea objetivo, autocrítico y realista.		
LMG	Sí, ya que como meta primordial el aseguramiento de la información debe de tomarse decisiones en cuanto a los mecanismos a implementar evaluando y comparando efectividad, durabilidad, permanencia, oportunidad en la implantación y costo, por lo que indudablemente es una labor de decisión.		
CRT			Sin comentarios

4.10 Cuestionario piloto (prueba).

4.10.1 Aplicación.

Este cuestionario fue aplicado a 4 personas involucradas en las áreas de tecnología informática general. Una de las personas cuestionadas, Victor Figueroa Peña, encargado de la administración de sistemas de la Tesorería de la Federación, forma parte de la muestra.

La aplicación del cuestionario se realizó con la finalidad de evaluar el nivel de comprensión del cuestionario; para que, en caso de que se requiera, se efectuarán ciertas adecuaciones a las preguntas y formar un cuestionario definitivo.

También se ha buscado determinar el tiempo que cada cuestionado en promedio requeriría para responder a todas y cada una de las preguntas.

Se encuentra una reproducción del cuestionario piloto aplicado en el anexo IV-1.

El cuestionario piloto se aplicó a las siguientes personas:

Rodolfo Reynoso B.
Empresa Integradores de Tecnología
Administración de IT

Víctor Figueroa Peña.
TESOFE
Administración de auditoria de sistemas.
(Contenido en la muestra).

Lic. Luis Martínez G.
Banamex.
División Productos de financiamiento Inmobiliario

Lic. Carlos Rey T.
Meta Data
Soporte técnico y puesta a punto.

4.10.2. Evaluación de la comprensión.

De los resultados obtenidos a través de la aplicación del cuestionario piloto se pudieron obtener las siguientes conclusiones:

Se puede afirmar que la comprensión de cada una de las preguntas del cuestionario resulta aceptable.

Se han incluido rangos de respuestas en las preguntas que no son abiertas, ello con la finalidad de interpretar, tratar y graficar de una mejor manera los resultados recopilados. Las preguntas modificadas son 1, 5, 6 y 8.

Otra finalidad de presentar de esta manera las preguntas es para proporcionar al usuario la impresión de no tener que apegarse exactamente a una respuesta contundente puntual y no tener selecciones entre una respuesta y otra.

La pregunta número 5 requiere un replanteamiento en la redacción. Ahora se aplicará una escala de respuestas en donde estará contenida parte de la redacción del cuestionario piloto.

4.10.3 Evaluación del tiempo de aplicación.

El tiempo necesario por los cuestionados para contestar todo el cuestionario fue aproximadamente entre 10 y 13 minutos con intervenciones de algún tópico por parte del autor.

4.11 Cuestionario definitivo.

El siguiente cuestionario se elaboró como parte de la investigación y el mismo se aplicó a cada uno de los integrantes de la muestra referida en "4.5 Determinación de la muestra".

El cuestionario toca temas relativos a la problemática ya tratada en las variables establecidas, y que fueron mencionadas anteriormente.

Como ya se ha indicado, algunas preguntas del cuestionario se han formulado no tan abiertas para proporcionar una mayor facilidad de respuesta al cuestionado, permitiendo (cuando se creyó conveniente) la ampliación de sus opiniones.

Se trató además que las preguntas estuvieran relacionadas lo mayormente posible, para obtener mejores resultados y poder así evaluar la hipótesis de trabajo.

La pregunta No. 7 se pudo haber convertido en una pregunta con opciones de respuestas múltiples seleccionables, sin embargo se deja abierta para detectar si las personas que conforman la muestra poseen o no el conocimiento del concepto "*servicios de seguridad*" referido en el marco problemático.

Se ha agregado una pregunta más -la pregunta número 9-, con la finalidad de saber si se han aplicado anteriormente estudios de seguridad como éste.

Una vez realizadas las observaciones y las adecuaciones anteriores, el cuestionario ha quedado tal y como se encuentra en el anexo IV-2.

4.12 Realización de la investigación.

El autor llevó a cabo la investigación acudiendo directamente a los centros de cómputo con las personas que integran la muestra. Se les presentó el cuestionario mostrado en el anexo IV-2 y brevemente se comentó el estado del arte del trabajo con la finalidad de proporcionar una introducción conceptual y con ello todos y cada uno de los cuestionados pudiesen comprender la problemática que hay detrás del instrumento de recopilación de información.

Además se les presentó una carta explicativa misma que se reproduce en el anexo IV-3 donde se expone el propósito de la investigación, extendiendo además una invitación para posteriormente conocer los resultados derivados de este trabajo.

El cuestionario definitivo se aplicó a las siguientes personas:

José A. Arellano Vargas.
Grupo Financiero Bancomer.
Administrador de la Base de Datos de Banca Empresarial.
Teléfono: 56-21-43-33
ENC_1

Ing. Alejandro Velázquez Mena.
Centro de Cómputo de la Facultad de Ingeniería.
Encargado de la administración interna y externa de la Facultad de Ingeniería de la UNAM.
Teléfono: 58-41-20-53
ENC_2

Ing. Rafael Pavón Sánchez.
Consultoría de Sistemas e-commerce S.A. de C.V.
Responsable de la organización operativa y de calidad y auditoria de proyectos.
Teléfono: 55-54-89-52

ENC_3

L.I. Nora Tapia.
Dirección de Cómputo para la Administración Académica.
Responsable de auditoria de sistemas.
Teléfono 56-22-75-49
ENC_4

Marisol Daza Alzaga.
Grupo Nacional Provincial.
Analista de calidad de sistemas.
ENC_5

Ing. David Silva.
Hussmann American.
Director de informática.
Teléfono: 58-04-19-39
ENC_6

Dr. Armando Perdomo.
IBM México.
Desarrollador de T.I.
Tel. 57-28-10-00 ext. 6942
ENC_7

Ing. Luis Enrique Pérez Molina.
InfoSyst S.A. de C.V. Miembro Fundador de AMITI (Asociación Mexicana de la Industria de Tecnologías de Información). Miembro de la Asociación Mexicana para la Calidad de Ingeniería de Software (AMCIS).
Director General.
Tel. 56-01-14-95 y 56-01-17-95
ENC_8

Victor Figueroa Peña.
Secretaría de Hacienda y Crédito público. TESOFE.
Administración de sistemas de información.
ENC_9

Resultados de la aplicación del cuestionario.

A continuación se resumen y analizan las respuestas proporcionadas por las personas a quienes se aplicó el cuestionario:

1.- ¿Cuenta su centro de cómputo con un plan de reducción de riesgos hecho con objetividad?

	No, nunca se ha hecho.	No, realmente en el centro de cómputo de la organización se da importancia a otras cuestiones menos a la seguridad en materia de cómputo.	Los planes de reducción de riesgos se hacen después de que se manifiesta un factor de riesgo.	Si se hacen planes de reducción de riesgos pero no hay profesionales que los hagan.	Si, los planes de reducción de riesgos son hechos con objetividad.
ENC_1					***
ENC_2				***	
ENC_3	***				
ENC_4					***
ENC_5			***	***	
ENC_6				***	
ENC_7					***
ENC_8			***		
ENC_9			***		

2.- Qué necesidades se han detectado en la organización derivadas de realizar estudios de *análisis de riesgos* y/o de seguridad?

ENC_1	Contar con personal capacitado en la materia para crear grupos de trabajo dedicados a proteger y resguardar principalmente la información.
ENC_2	Instalar parches en los sistemas operativos y en las aplicaciones. Se han detectado además colocar medidas más estrictas para que los usuarios no utilicen el equipo de cómputo para otros fines distintos de los académicos. Otra necesidad detectada es que la seguridad es un tema que debe tenerse muy actualizado.
ENC_3	Ninguno, pues no se ha llevado a cabo ningún tipo de estudio de riesgos.
ENC_4	Especialización de personal para realizar labores de *análisis de riesgos* y auditoria en cada una de las etapas de un sistema de software,
ENC_5	Mayor seguridad en las entradas y salidas de activos, así como también mayor seguridad en la entrada y salida de información vía correo electrónico, discos, etc.
ENC_6	Específicamente necesidades de herramientas en comunicaciones remotas. Otros riesgos relacionados con el suministro de corriente eléctrica, almacenaje, fuego, accesos, etc. Están "bajo control".
ENC_7	La creación de un equipo de personas dedicado a los factores de seguridad (e inseguridad) centro del centro de cómputo.

ENC_8	Necesidades de compra de equipo, dispositivos, posiblemente la creación de algún sistema de monitoreo en los pasillos, oficinas, etc.
ENC_9	Solo se contemplan riesgos evidentes, considero que las áreas dedicadas a la seguridad informática no están tan involucradas en el desarrollo como para poder completar estudios fieles.

3.- ¿Cómo se cuantifican los riesgos a los cuales están sujetos los activos cuando se realiza un *análisis de riesgos* o un estudio de seguridad?

ENC_1	Se toma en cuenta el costo ($), tiempo de recuperación, horas-hombre perdidas, etc.
ENC_2	La manera más sencilla de hacerlo es cuantificarlos de manera económica, porque también podrían cuantificarse por el daño generado, por el tiempo de latencia o por un número n de posibles cuantificadores.
ENC_3	No se lleva a cabo.
ENC_4	Con un grado de severidad o bien monetario (económico).
ENC_5	Económicamente.
ENC_6	En base a la incidencia histórica y a una estimación burda.
ENC_7	Principalmente se toma en cuenta el tipo de riesgo y se cuantifica en costo económico y humano.
ENC_8	Económicamente.
ENC_9	Considero que no están cuantificados, solo se detectan los más evidentes y se hacen "estrategias" sin objetivos, ni la aplicación de soluciones. Evidentemente por la falta de contacto con el área de desarrollo.

4.- ¿ Cómo se estima la probabilidad de ocurrencia de cada riesgo después de haber realizado un *análisis de riesgos* o un estudio de seguridad?

ENC_1	Generalmente en base a experiencias previas tanto dentro de la organización como de casos externos conocidos.
ENC_2	Se analiza el escenario en donde ocurrió ese riesgo y se simulan nuevamente esos escenarios de peligro para ver que tan factible sería el que volviese a ocurrir un atentado contra la seguridad.
ENC_3	¿?
ENC_4	Depende hay riesgos que son muy difíciles de evaluar dado que para que ocurran debería de tratarse de una condición excepcional. En otros casos los incidentes de seguridad son tan comunes que ya hasta pasan inadvertidos (como la perdida de un disco floppy o el préstamo de una clave de acceso), sin embargo también deberían considerarse las probabilidades de ocurrencia.
ENC_5	Mediante procesos estadísticos.
ENC_6	En cada caso es diferente: Corriente eléctrica.- Incidencia histórica. Almacenamiento.- Parámetros nominales del proveedor junto con referencias de otros usuarios. Fuego.- Se establece una muy alta probabilidad. Terremotos.- Se establece una muy baja prioridad. Accesos.- Se establece una probabilidad del 100 % del riesgo.
ENC_7	En base a experiencias pasadas dentro del centro de cómputo.
ENC_8	Aún no hemos hecho eso. Se podría estimar empíricamente, no existe un documento que lo indique formalmente.
ENC_9	No esta estimado o no se ha difundido lo necesario

5.- ¿Cómo permanecen los controles de seguridad ya existentes después de realizar un *análisis de riesgos* o un estudio de seguridad?

	No existen controles de seguridad.	No se toma ninguna referencia de controles de seguridad previos a pesar de existir.	Se toman como referencia los controles de seguridad previos pero se mantienen inalterables.	Los controles de seguridad son modificados.	Se generan nuevos planes de mitigación de riesgos y planes de corrección y prevención de accidentes.
ENC_1				***	***
ENC_2					***
ENC_3			***		
ENC_4					***
ENC_5					***
ENC_6				***	
ENC_7				***	***
ENC_8		***			
ENC_9	***				

6.- ¿La asignación de recursos humanos, financieros y/o materiales se ve modificada cuando se realiza un *análisis de riesgos* o un estudio de seguridad?

	No, no hay voluntad gerencial.	No a pesar de haber interés gerencial	No ha sido necesario hasta este momento.	Sí, a pesar de no haber inicialmente voluntad gerencial.	Sí, el interés sobre el área de seguridad de la empresa es muy importante.
ENC_1					***
ENC_2		***			
ENC_3			***		
ENC_4				***	
ENC_5					***
ENC_6				***	
ENC_7				***	
ENC_8				***	
ENC_9			***		

7.- Cuando se realiza un *análisis de riesgos* y/o un estudio de seguridad en el centro de cómputo, ¿se pueden detectar los *servicios de seguridad* que tienen los procesos que utilizan la información?

ENC_1	Si porque hay (debe haber) registros que indican tales procesos, y deben ser tomados en cuenta por quienes manejan la información.
ENC_2	Si, ello se puede llevar a cabo por medio de software, hardware, controles humanos, controles mecánicos, electrónicos, etc. etc.
ENC_3	Si, imagino que debe ser así.
ENC_4	Si.
ENC_5	Si, si se pueden detectar.
ENC_6	Si.
ENC_7	Si, debido a que existe un registro previo de algún otro percance y en base a esto se han hecho respaldos de la información que pudiera ser dañada.
ENC_8	Si.
ENC_9	Al parecer los procesos que utilizan la información no tienen *servicios de seguridad*.

Nota: En el campo de las ciencias de la computación en ocasiones se encuentra que hay términos mal definidos y que son utilizados por distintos autores de forma conflictiva, y a veces claramente contradictorios. Esta pregunta se aplicó a cada una de las personas que integran la muestra y se encontró que efectivamente tal y como se indica en "4.11 Cuestionario definitivo", la mayoría de ellas desconoce la definición real de un "*servicio de seguridad*".

Se ha vuelto a aplicar esta pregunta pero dando una explicación breve sobre lo que en este trabajo significa "*servicio de seguridad*". Los datos obtenidos en esta pregunta se recopilaron por medio de llamadas telefónicas.

Teniendo en cuenta que, un *proceso* es un "conjunto de técnicas que permiten almacenar datos, tener acceso a ellos y combinarlos con vistas a su utilización" [44]

Y que, de acuerdo a la arquitectura de seguridad *OSI* existen cinco *servicios de seguridad*:

Servicios de *autenticación*. Proporcionan *autenticación* en el proceso de comunicación entre dos entidades o para la *autenticación* del origen de datos.
Servicios de *control de acceso*. Utilizados para proteger los recursos del sistema contra su utilización no autorizada. Estos servicios están estrechamente relacionados con los servicios de *autenticación*.
Servicios de *confidencialidad* de los datos. Protegen a los datos de revelaciones no autorizadas.
Servicios de *integridad* de los datos. Protegen a los datos de modificaciones no autorizadas.

[44] Definición de proceso según Diccionario Enciclopédico Hachette Castell
ISBN 84-7489-169-8 (tomo IX)
Ediciones Castell 1981

Servicios de *no repudio*. Proporcionan cierta protección contra el remitente de un mensaje o acción que niega serlo, o contra el receptor de un mensaje que niega haberlo recibido.
La pregunta Número 7 se modificó y se aplicó de la siguiente manera:

7.- Cuando se realiza un *análisis de riesgos* y/o un estudio de seguridad en su centro de cómputo, ¿se pueden detectar en los procesos que utilizan la información, los siguientes *servicios de seguridad*:
Servicios de *autenticación*.
Servicios de *control de acceso*.
Servicios de *confidencialidad* de los datos.
Servicios de *integridad* de los datos y/o
Servicios de *no repudio*.

ENC_1	Si, en realidad en el área en la que me desarrollo el sistema administrador de la base de datos ya tiene de manera implícita varios de los *servicios de seguridad*, la *autenticación* y los controles de acceso son aplicados cuando un usuario ya sea de administración o de usuario no administrador intenta por vez primera accesar en el sistema durante una sesión, además también de manera implícita el *RDBMS* establece las normas que garanticen que los datos contenidos en la base de datos se mantengan íntegros.
ENC_2	Sí, generalmente lo que se lleva a cabo en toda herramienta de seguridad que es instalada es consultar los archivos de bitácoras o los reportes que son enviados a la pantalla en donde se indica si los *servicios de seguridad* mencionados son vulnerables o no.
ENC_3	Sí, imagino que debe ser así.
ENC_4	Sí, aunque el servicio de *no repudio* no.
ENC_5	Sí, son detectables incluso antes de hablar de procesos, es decir, antes de que un proceso sea liberado como tal, deben de estar soportados en servicios que garanticen que la ejecución del flujo normal del proceso no se vea afectada por ningún tipo de eventualidad que pudiese afectar la *confidencialidad* de los datos o la *autenticación* de los usuarios en los sistemas.
ENC_6	Sí, aunque todo se hace con software, inclusive los servicios de *no repudio* se llevan a cabo con tecnologías criptográficas de *llave* pública.
ENC_7	Sí.
ENC_8	Sí.. Dado que en el centro de cómputo se labora en ambientes de red, todos los usuarios antes de hacer uso de un recurso deben identificarse ante la computadora. El *control de acceso* a los recursos también esta previsto. La *confidencialidad* de los datos depende de cada usuario. El *no repudio* no es aplicable.
ENC_9	Sí, se cuenta con *autenticación*, controles de acceso físico y lógico,

	datos sensibles (importantes) se encuentran en respaldos y disponibles en todo momento. Para garantizar que alguien ha realizado una acción hay varios controles que van desde identificaciones impresas hasta uso de software criptográfico

8.- ¿El realizar un *análisis de riesgos* permite establecer las bases para una toma de decisiones en su organización?

	Sí	No.	Lo desconozco.
ENC_1	***		
ENC_2		***	
ENC_3	***		
ENC_4	***		
ENC_5	***		
ENC_6	***		
ENC_7	***		
ENC_8	***		
ENC_9	Si, ya que como meta primordial el aseguramiento de la información debe de tomarse decisiones en cuanto a los mecanismos a implementar evaluando y comparando efectividad, durabilidad, permanencia, oportunidad en la implantación y costo, por lo que indudablemente es una labor de decisión.		

9.- ¿Anteriormente había sido cuestionado con preguntas como éstas?

	SI.	No.
ENC_1	***	
ENC_2	***	
ENC_3		***
ENC_4	***	
ENC_5	***	
ENC_6	***	
ENC_7		***
ENC_8		***
ENC_9		***

Estos resultados también pueden observarse en el anexo IV-4.

4.13 Tratamiento sistematizado de la información.

Tratamiento para la pregunta 1.

¿Cuenta su centro de cómputo con un plan de reducción de riesgos hecho con objetividad?

Sí, son hechos con objetividad.....0.3
Sí, pero por gente no caificada.....0.3
Sí, se realizan pero sólo hasta que se manifiesta un factor de riesgo.....0.3
No, nunca se han hecho.....0.1

1.0

Tratamiento para la pregunta 2.

¿Qué necesidades se han detectado en la organización derivadas de realizar estudios de *análisis de riesgos* y/o de seguridad?

De todos los factores mencionados por los cuestionados se tienen las siguientes respuestas:

Necesidad de contar con personal capacitado-calificado.....0.25
Necesidad de contar con un mejoramiento en la seguridad de las comunicaciones.....0.17
Ninguna.....0.17
Obtención de software para corregir software (parches, servicepacks, actualizaciones, etc).....0.08
Creación de reglamentos.....0.08
Necesidad de ver a la seguridad como un tema prioritario en su flujo de negocio.....0.08
Implementación de un sistema efectivo de seguridad en los accesos físicos.....0.08
Detección de una falta de dispositivos de vigilancia.....0.08

0.99

Tratamiento para la pregunta 3.

¿Cómo se cuantifican los riesgos a los cuales están sujetos los activos cuando se realiza un *análisis de riesgos* o un estudio de seguridad?

En base a lo que costaría el que se manifestase el factor de riesgo.....0.46
Otros.....0.24

Se realiza una cuantificación empírica.....0.15
En base a lo que costaría en términos de tiempo el reponerse de la manifestación del factor de riesgo.....0.07
No se lleva a cabo 0.07

0.99

Tratamiento para la pregunta 4.

¿Cómo se estima la probabilidad de ocurrencia de cada riesgo después de haber realizado un *análisis de riesgos* o un estudio de seguridad?

En base a estimaciones históricas de referencia.....0.33
No sabe.....0.33
Otros (procesos estadísticos, asignación de porcentajes empíricos, etc.).....0.22
Reproducción de escenarios de riesgo.....0.11

0.99

Tratamiento para la pregunta 5.

¿Cómo permanecen los controles de seguridad ya existentes después de realizar un *análisis de riesgos* o un estudio de seguridad?

Se generan nuevamente planes de contingencia y prevención de riesgos.....0.45
Son modificados los controles de seguridad existentes.....0.27
Se toman como referencias pero no se llevan a cabo modificaciones.....0.09
No se toma ninguna referencia de los controles existentes.....0.09
No existen controles de seguridad.....0.09

0.99

Tratamiento para la pregunta 6.

¿La asignación de recursos humanos, financieros y/o materiales se ve modificada cuando se realiza un *análisis de riesgos* o un estudio de seguridad?

Sí, a pesar de no haber voluntad gerencial inicialmente	0.44
Sí, hay bastante interés	0.22
No ha sido necesario hasta el momento	0.22
No, a pesar de haber interés gerencial	0.11
	0.99

Tratamiento para la pregunta 7.

Cuando se realiza un *análisis de riesgos* y/o un estudio de seguridad en su centro de cómputo, ¿se pueden detectar en los procesos que utilizan la información, los siguientes *servicios de seguridad*:

Servicios de *autenticación.*
Servicios de *control de acceso.*
Servicios de *confidencialidad* de los datos.
Servicios de *integridad* de los datos y/o
Servicios de *no repudio.*

Sí	1.0
No	0.0
	1.0

Tratamiento para la pregunta 8.

¿El realizar un *análisis de riesgos* permite establecer las bases para una toma de decisiones en su organización?

Sí	0.88
No	0.11
	0.99

Nadie lo desconoce, todos están conscientes que el realizar un *análisis de riesgos* puede o no puede establecer las bases para una toma correcta de decisiones.

Tratamiento para la pregunta 9.

¿Anteriormente había sido cuestionado con preguntas como éstas?

Sí	0.55
No	0.44
	0.99

4.14 Análisis de los resultados.

1/10 de la muestra no cuenta con un plan de reducción de riesgos, no únicamente hecho con objetividad, sino que nunca lo ha realizado.

3/10 de la muestra realizan planes de reducción de riesgos hechos con objetividad pero hasta que se hace presente un factor de riesgo.

6/10 (3/5) de la muestra si realizan planes de reducción de riesgos hechos con objetividad, pero, de éstos el 50% (3/10) son realizados por gente no capacitada.

Los cuestionados llevan a cabo planes de reducción de riesgos, el 0.9 de las respuestas así lo indican, sin embargo, lo que se busca con esta pregunta no es saber si se llevan a cabo o no, sino que si son realizados con objetividad, con formalidad, con calidad, para lo cual el porcentaje se reduce a 0.3. No se podrían considerar planes objetivos aquellos realizados por personas sin preparación especializada en materia de riesgos computacionales. Tampoco podrán considerarse como planeas fiables aquellos que son generados por la ocurrencia de un siniestro el cual no se había previsto anteriormente, ello reflejaría la falta de interés en el tema.

El 0.75 de los cuestionados declaró el haber detectado alguna necesidad en la organización en la que labora, derivado de realizar un *análisis de riesgos* y/o de seguridad.

Curiosamente el porcentaje que indica que no se ha detectado ninguna necesidad en la organización derivada de realizar un estudio de *análisis de riesgos* y/o de seguridad ocupa la misma frecuencia en contestaciones que la necesidad detectada de contar con mejoramientos en las comunicaciones, 2ª., en orden de contestación, y casi el doble de contestaciones con respecto a la creación de reglamentos o la seguridad necesaria en los accesos físicos.

La necesidad primaria, efectivamente, la constituye el recurso humano, desafortunadamente la escasez del experto en esta área es una realidad palpable. [45]

El 0.92 de los cuestionados cuantifican los riesgos a los cuales están sujetos los activos cuando se realiza un *análisis de riesgos* o un estudio de seguridad.

El mayor porcentaje (casi la mitad de las contestaciones) cuantifican los riesgos a los cuales están sujetos los activos en base a lo que costaría el que se manifestase el factor de riesgo.

La probabilidad de ocurrencia de cada riesgo después de haber realizado un *análisis de riesgos* o un estudio de seguridad se hace mayoritariamente en dos vertientes: la primera en base a estimaciones históricas de referencia, la segunda, curiosamente no saben.

El realizar un *análisis de riesgos* provoca la creación de nuevos planes de contingencia y de prevención de riesgos.

Curiosamente, la muestra esta conformada por empresas que tienen muy buena reputación en general, sin embargo es posible encontrar dentro de la muestra aquellas en las que no existen controles de seguridad, entonces qué es lo que hay que esperar en empresas de talla más pequeña?

La asignación de recursos humanos, financieros y/o materiales en ocasiones no se modifica cuando se realiza un *análisis de riesgos* o un estudio de seguridad.

Si las respuestas obtenidas son tratadas con una media aritmética se tendría lo siguiente:

Cuestionados que respondieron que sí se daban modificaciones en las asignaciones de recursos: □□□x/n = 6/9 = 0.66
Cuestionados que respondieron negativamente: □□□x/n = 3/9 = 0.33

[45] Haga una reflexión y pregúntese si en el centro de cómputo en donde usted labora existe personal especializado en el área de seguridad.

Absolutamente nadie contesto que no había voluntad gerencial para no hacerlo.

El 100 % de la muestra, después de rediseñar la pregunta número 7 relacionada con los *servicios de seguridad* aseveran que cuando se realiza un *análisis de riesgos* y/o un estudio de seguridad en su centro de cómputo, sí se pueden detectar en los procesos que utilizan la información, los siguientes *servicios de seguridad*:

Servicios de *autenticación*.
Servicios de *control de acceso*.
Servicios de *confidencialidad* de los datos.
Servicios de *integridad* de los datos y/o
Servicios de *no repudio*.

El 0.88 concuerda con que realizar un *análisis de riesgos* permite establecer las bases para una toma de decisiones de las organizaciones.

El 0.55 ha declarado que ya ha contestado cuestionarios parecidos, lo que quiere decir que ya se esta trabajando al respecto en este campo, sin embargo aún es muy bajo ese porcentaje, además hay que recordar que en muchas ocasiones la gente que se dedica a la administración o auditoria de computadoras y ambientes de red carecen de los conocimientos necesarios para poder considerarse como profesional del tema.

4.15 Aprobación o desaprobación de la hipótesis.

Para la aprobación de la hipótesis planteada, se hará una revisión de las variables dependientes e independientes que se han señalado en "4.1. Variables", cotejándolas con los resultados de la investigación.

4.15.A. Variable independiente (presentación del problema en su causa):

Si un centro de cómputo realiza un análisis de los riesgos que afectan a la información que captan, procesan, despliegan, distribuyen y/o almacenan.

4.15.B. Variables dependientes (presentación del problema en sus efectos):

Se puede crear un plan de reducción de riesgos con objetividad.

Conclusión.- Sí, si se crean planes de reducción de riesgos, ellos son realizados por distintos tipos de personas, los planes de reducción de riesgos realizados con objetividad no los deberían crear el personal con deficiencias de conocimiento en el tema, sino que deberían de ser realizados por personas profesionales en el campo. Por lo tanto no puede considerarse como un plan objetivo a aquel que es realizado por personas sin los conocimientos necesarios ni por el personal que una vez pasado el factor de riesgo trate de crear un plan de mitigación.
El porcentaje de cuestionados que indicó que los planes de reducción de riesgos son objetivos (y que llevan a cabo planes de reducción de riesgos) tan sólo es del 0.30.

Para este caso se tomará una variable interviniente: el tipo de personal que realiza los planes de reducción de riesgos. Ya se ha establecido que la diversidad en el tipo de personal que realiza estas actividades cuenta con conocimientos heterogéneos en el tema de seguridad computacional. Entonces, si consideramos que las personas que realizan los planes de reducción de riesgos no son gente experta en el tema esta variable dependiente no se podría tomar como válida, no por la falta de riqueza de la variable, sino porque no hay gente que pueda realizarlos planes de riesgos con objetividad, sin embargo si las personas que realizan los planes de reducción de riesgos si son gente experta en el tema esta variable dependiente sí se toma como válida.

Esta variable dependiente se toma como válida por la acción de la variable interviniente.

Se pueden determinar algunas necesidades no detectadas en la empresa.

Conclusión.- Efectivamente, más del 0.8 así lo han indicado, la necesidad primaria la constituye el factor humano con conocimientos especializados, la segunda necesidad detectada la constituyen las transmisiones en ambientes de redes de computadoras.
Esta variable dependiente se toma como válida.

Se pueden cuantificar los riesgos a los cuales están sujetos los activos.

Conclusión.- El 0.92 de los cuestionados cuantifican los riesgos a los cuales están sujetos los activos cuando se realiza un *análisis de riesgos* o un estudio de seguridad. La cuantificación económica es el principal tipo seguida de otros, las cuantificaciones con respecto al tiempo en el que tardaría en restablecerse el flujo normal de as operaciones donde se hizo presente el factor de riesgo cae por debajo de éstas.
Esta variable dependiente se toma como válida.

Se puede estimar la probabilidad de ocurrencia de cada riesgo latente.

Conclusión.- El 0.66 de los cuestionados estiman la probabilidad de ocurrencia de cada riesgo latente. El mayor porcentaje lo realiza con respecto a estimaciones históricas.
Esta variable dependiente se toma como válida.

Se pueden revisar y redefinir los controles de seguridad ya existentes.

Conclusión.- El 0.72 de los cuestionados revisan, redefinen y hasta generan nuevos controles de seguridad a partir de los existentes.
Esta variable dependiente se toma como válida.

Se pueden asignar para su estudio pocos recursos tanto humanos, financieros y/o materiales.

Conclusión.- El 0.66 de los cuestionados realizan una reasignación de los recursos necesarios tanto humanos, financieros y/o materiales a pesar de que inicialmente no se contaba con la voluntad gerencial.
Esta variable dependiente se toma como válida.

Se pueden conocer los *servicios de seguridad* con que cuentan los procesos que la utilicen (a la información).

Conclusión.- Así es.
Esta variable dependiente se toma como válida.

Se pueden establecer bases para una toma de decisiones.
Conclusión.- El 0.88 de los cuestionados así lo detecta.
Esta variable dependiente se toma como válida.

Por lo anterior se puede concluir que la hipótesis se aprueba de manera total, aunque existe la agregación en la redacción de la hipótesis de una variable interviniente.

La hipótesis resultante derivada de la aplicación de esta investigación sufre una pequeña adecuación en la redacción, enseguida se reproduce la hipótesis de trabajo y enseguida la hipótesis modificada:

Hipótesis de trabajo:

"Si un centro de cómputo realiza análisis de los riesgos que afectan a la información que captan, procesan, despliegan, distribuyen y/o almacenan entonces se pueden crear planes de reducción de riesgos objetivos, se pueden determinar algunas necesidades no detectadas en la empresa, se pueden cuantificar los riegos a los cuales están sujetos los activos, se puede estimar la probabilidad de ocurrencia de cada riesgo latente, se pueden revisar y redefinir los controles de seguridad ya existentes, se pueden asignar para su estudio pocos recursos tanto humanos, financieros y/o materiales, se pueden conocer los servicios de seguridad con que cuentan los procesos que la utilicen (a la información) y se pueden establecer bases para una toma de decisiones".

Hipótesis modificada por la agregación de la variable interviniente:

"Si personal capacitado[46] de un centro de cómputo, con los conocimientos adecuados en materia de seguridad computacional, realiza un análisis de los riesgos que afectan a la información que se capta, procesa, despliega, distribuye y/o almacena en el centro de cómputo, entonces se pueden determinar algunas necesidades no detectadas en la organización, se pueden cuantificar los riegos a los cuales están sujetos los activos, se puede estimar la probabilidad de ocurrencia de cada riesgo latente, se pueden revisar y redefinir los controles de seguridad ya existentes, se pueden asignar para su estudio pocos recursos tanto humanos, financieros y/o materiales, se pueden conocer los servicios de seguridad con que cuentan los procesos que la utilicen (a la información) y se pueden establecer bases para una toma de decisiones".

4.16 Conclusiones.

En este capítulo se pudieron obtener varias conclusiones:

- Los análisis de riesgos son realizados por distintos tipos de personas, con o sin conocimientos de seguridad en cómputo. El porcentaje de personas que realizan análisis de riesgos sin conocimientos es mucho mayor que el porcentaje de personas preparadas que lo realizan.
- Se pueden determinar algunas necesidades no detectadas en la empresa.
- Se pueden cuantificar los riesgos a los cuales están sujetos los activos.
- Se puede estimar la probabilidad de ocurrencia de cada riesgo latente.
- Se pueden revisar y redefinir los controles de seguridad ya existentes.
- Se pueden asignar para su estudio pocos recursos tanto humanos, financieros y/o materiales.
- Se pueden conocer los *servicios de seguridad* con que cuentan los procesos que la utilicen (a la información).
- Se pueden establecer bases para una toma de decisiones.
- Se toma como válida a la hipótesis de trabajo.

[46] Entiéndase como personal capacitado aquel que posee los conocimientos teóricos y prácticos adecuados y suficientes en materia de seguridad computacional, que conozca los atacantes potenciales, sus objetivos, los accesos físicos y lógicos por los cuales se podría manifestar un percance, los resultados que se podrían derivar en caso de que se presentase un factor de riesgo, las herramientas que un atacante podría utilizar y las medidas correctivas en caso de que un riesgos se hiciese presente.

4.17 Anexos.

4.17.A. Anexo IV-1 Cuestionario piloto.

¿Cuenta su centro de cómputo con un plan de reducción de riesgos hecho con objetividad?

¿Qué necesidades se han detectado en la organización derivadas de realizar estudios de *análisis de riesgos* y/o de seguridad?

¿Cómo se cuantifican los riesgos a los cuales están sujetos los activos cuando se realiza un *análisis de riesgos* o un estudio de seguridad?

¿ Cómo se estima la probabilidad de ocurrencia de cada riesgo después de haber realizado un *análisis de riesgos* o un estudio de seguridad?

¿Cómo permanecen los controles de seguridad ya existentes después de realizar un *análisis de riesgos* o un estudio de seguridad?, ¿inalterables?, ¿si son modificados?

¿La asignación de recursos humanos, financieros y/o materiales se ve modificada cuando se realiza un *análisis de riesgos* o un estudio de seguridad?

Cuando se realiza un *análisis de riesgos* y/o un estudio de seguridad en el centro de cómputo, ¿se pueden detectar los *servicios de seguridad* que tienen los procesos que utilizan la información?

¿El realizar un *análisis de riesgos* permite establecer las bases para una toma de decisiones en su organización?

4.17.B. Anexo IV-2 Cuestionario definitivo.

Fecha: _____
Nombre: _____
Puesto: _____
Empresa: _____
Contacto (teléfono, email, dirección, etc.): _____

¿Cuenta su centro de cómputo con un plan de reducción de riesgos hecho con objetividad?
____ No, nunca se ha hecho.
____ No, realmente en el centro de cómputo de la organización se da importancia a otras cuestiones menos a la seguridad en materia de cómputo.
____ Los planes de reducción de riesgos se hacen después de que se manifiesta un factor de riesgo.
____ Si se hacen planes de reducción de riesgos pero no hay profesionales que los hagan.
____ Si, los planes de reducción de riesgos son hechos con objetividad.

¿Qué necesidades se han detectado en la organización derivadas de realizar estudios de *análisis de riesgos* y/o de seguridad?

_____
_____
_____

¿Cómo se cuantifican los riesgos a los cuales están sujetos los activos cuando se realiza un *análisis de riesgos* o un estudio de seguridad?

_____
_____
_____

¿ Cómo se estima la probabilidad de ocurrencia de cada riesgo después de haber realizado un *análisis de riesgos* o un estudio de seguridad?

_____
_____
_____

¿Cómo permanecen los controles de seguridad ya existentes después de realizar un *análisis de riesgos* o un estudio de seguridad?
____ No existen controles de seguridad.
____ No se toma ninguna referencia de controles de seguridad previos a pesar de existir.
____ Se toman como referencia los controles de seguridad previos pero se mantienen inalterables.
____ Los controles de seguridad son modificados.
____ Se generan nuevos planes de mitigación de riesgos y planes de corrección y prevención de accidentes.

¿La asignación de recursos humanos, financieros y/o materiales se ve modificada cuando se realiza un *análisis de riesgos* o un estudio de seguridad?
____ No, no hay voluntad gerencial.
____ No a pesar de haber interés gerencial
____ No ha sido necesario hasta este momento.
____ Sí, a pesar de no haber inicialmente voluntad gerencial.
____ Sí, el interés sobre el área de seguridad de la empresa es muy importante.

7. Cuando se realiza un *análisis de riesgos* y/o un estudio de seguridad en su centro de cómputo, ¿se pueden detectar en los procesos que utilizan la información, los siguientes *servicios de seguridad*:
Servicios de *autenticación*.
Servicios de *control de acceso*.
Servicios de *confidencialidad* de los datos.
Servicios de *integridad* de los datos y/o
Servicios de *no repudio*.

8. ¿El realizar un *análisis de riesgos* permite establecer las bases para una toma de decisiones en su organización?
____ Sí.
____ No.
____ Lo desconoce.

¿Anteriormente había sido cuestionado con preguntas como éstas?
____ Sí.
____ No.

Comentarios:_____
_____
_____
Observaciones: _____
_____
_____
_____

Firma: _____

4.17.C. Anexo IV-3 Carta de presentación.

Fecha: 7 de agosto del 2000.

A quien corresponda.

Presente.

Por medio de la presente me permito someter a su amable consideración la solicitud para obtener el permiso de aplicar un cuestionario de 9 preguntas a la persona o personas responsables de la seguridad y/o auditoria de su centro de cómputo con la finalidad de culminar un trabajo de investigación de tipo tesis profesional.

Desde el momento de recibir la información se utilizará en todos los casos con un grado razonable de cuidado para evitar la revelación y proteger la *confidencialidad* de la información escrita recibida y la información oral o visual identificada

La divulgación de los resultados globales se llevará a cabo por medio del trabajo de tesis mismos que se harán llegar a usted para su conocimiento.

Cualquier dato adicional o aclaración tendré mucho agrado en proporcionarla.

El tesista investigador firma al calce para efectos de identificación.

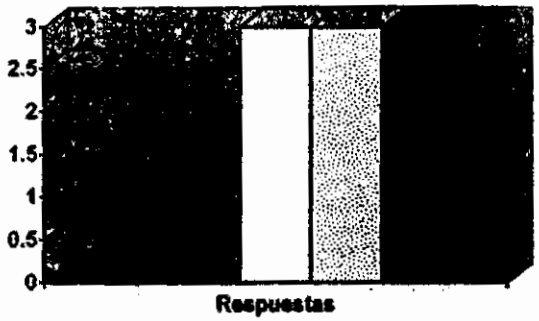
Agradeciendo su apoyo le saludo atentamente.

Victor López Guerrero
No. de cta. de la UNAM: 9128638-1
Tel. casa: 56 97 35 81
Tel. oficina: 56 01 14 95

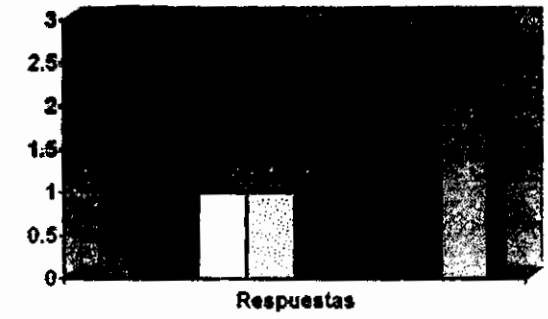
Dr. Ricardo Rivera Soler
Tel. oficina. 55 98 76 21
Tel. casa. 56 76 62 86

4.17.D. Anexo IV-4 Conclusiones derivadas de la aplicación de los cuestionarios objeto de la investigación.

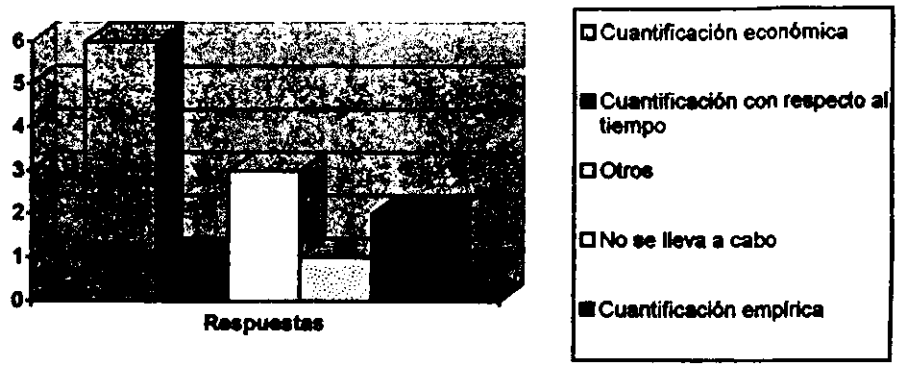
Respuestas para la pregunta 1.
1.- ¿Cuenta su centro de cómputo con un plan de reducción de riesgos hecho con objetividad?



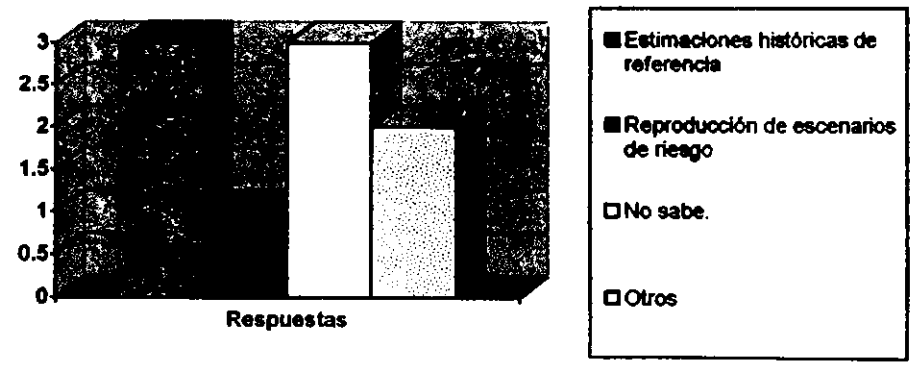
Respuestas para la pregunta 2.
2.- Qué necesidades se han detectado en la organización derivadas de realizar estudios de *análisis de riesgos* y/o de seguridad?



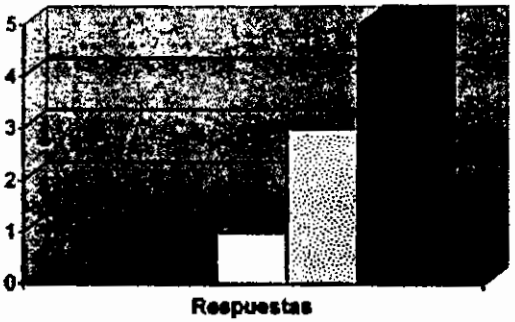
3.- ¿Cómo se cuantifican los riesgos a los cuales están sujetos los activos cuando se realiza un *análisis de riesgos* o un estudio de seguridad?



4.- ¿ Cómo se estima la probabilidad de ocurrencia de cada riesgo después de haber realizado un *análisis de riesgos* o un estudio de seguridad?

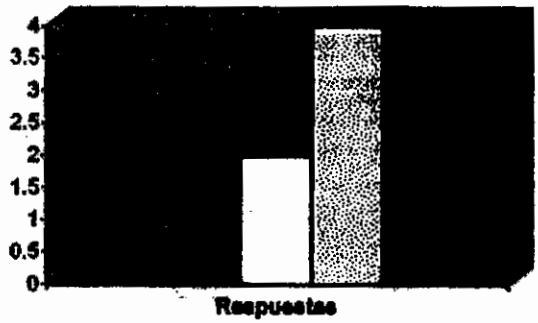


5.- ¿Cómo permanecen los controles de seguridad ya existentes después de realizar un *análisis de riesgos* o un estudio de seguridad?



- No existen controles de seguridad
- No se toma ninguna referencia
- Se toman referencias pero se mantienen inalterables.
- Los controles de seguridad son modificados.
- Se generan planes de contingencia y prevención de riesgos.

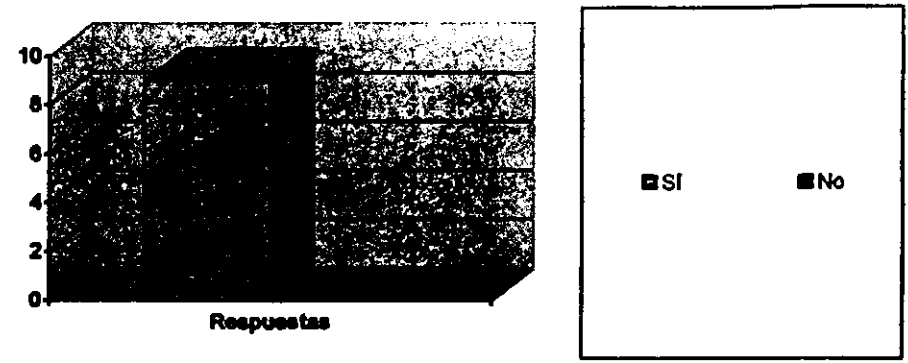
6.- ¿La asignación de recursos humanos, financieros y/o materiales se ve modificada cuando se realiza un *análisis de riesgos* o un estudio de seguridad?



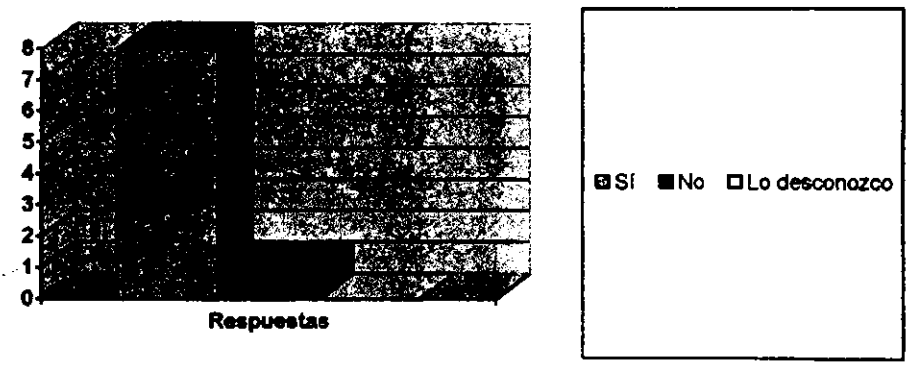
- No, no hay voluntad gerencial.
- No, a pesar de haber interés gerencial.
- No ha sido necesario hasta el momento.
- Sí, a pesar de no haber voluntad gerencial inicialmente.
- Sí, el interés es demasiado.

7.- Cuando se realiza un *análisis de riesgos* y/o un estudio de seguridad en su centro de cómputo, ¿se pueden detectar en los procesos que utilizan la información, los siguientes *servicios de seguridad*:

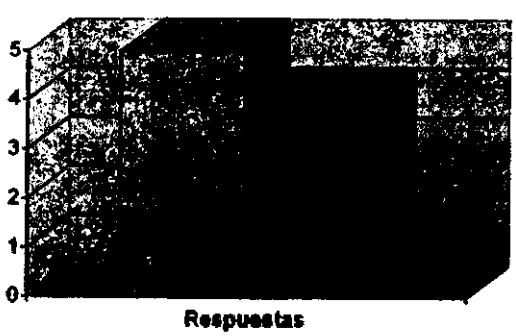
Servicios de *autenticación*.
Servicios de *control de acceso*.
Servicios de *confidencialidad* de los datos.
Servicios de *integridad* de los datos y/o
Servicios de *no repudio*.

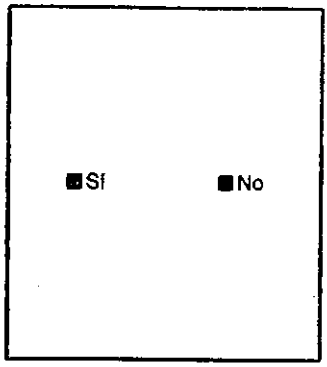


8.- ¿El realizar un *análisis de riesgos* permite establecer las bases para una toma de decisiones en su organización?



9.- ¿Anteriormente había sido cuestionado con preguntas como éstas?





4.18. Referencia bibliográfica.

Estadística para administración y economía.
Mendenhall y Reinmuth
Grupo editorial Iberoamérica.
México 1981
3ª. Edición.
ISBN 968-7270-13-6

V. MARCO INSTRUMENTAL.

5.1. Propuestas de acción.

Las propuestas de acción son los caminos que atienden a la difusión de los resultados de la investigación.

Las propuestas de acción a seguir para difundir el presente trabajo de investigación son las siguientes:

1. Publicación en:
   - Revistas.
   - Internet.
2. Ofertamiento personal para presentar conferencias en eventos relacionados con la informática.
3. Inclusión en la currícula académica, pudiendo ser:
   - Temática en la materia "Administración de centros de cómputo" impartida en noveno semestre de la licenciatura en informática.
   - Temática en la materia "Auditoria informática" impartida en décimo semestre de la licenciatura en informática.
   - Integral como materia optativa con la posible denominación de "Seguridad en computadoras y redes de computadoras" enfocada a los alumnos de semestres terminales de la licenciatura en informática.
   - Integral dándole un enfoque meramente informativo en vez de un enfoque matemático tal y como se ha venido dando con la materia "criptografía y seguridad" impartida en 10°. Semestre en la licenciatura en informática. De hecho un apartado de la materia propuesta esta enfocado a la criptografía.
4. Divulgación para crear cursos en empresas dedicadas a la educación.

En 5.2 se presentan el plan y programa de trabajo para cada una de las propuestas anteriores.

5.2 Plan y programa de trabajo.

5.2.A. Publicaciones.

Publicación en:
- Revistas.
- Internet.

Se ha tratado de publicar un artículo basado en el marco conceptual en las siguientes publicaciones:

PC Computing.
Contactos: Ivette Cervantes V. Y Arlette González D
e-mail: pc.computing@siedi.spin.com.mx

Universo de la computación.
Periódico "El Universal"
http://www.el-universal.com.mx
correo: univcomp@aguila.el-universal.com.mx

Gaceta UNAM y UNAM Hoy
dginfo@condor.dgsca.unam.mx
56230401, 56230401, 56230420

Publicaciones UNAM
Dirección General de Publicaciones y Fomento Editorial.
pfedico@servidor.unam.mx

Periódico Humanidades
http://biblioweb.dgsca..unam.mx/humanidades

Los Universitarios.
cazes@servidor.unam.mx

ciencias
biblat@selene.cichcu.unam.mx

Pero hasta el momento ninguna de ellas ha accedido a tal petición.

Internet:

Se puede consultar en línea un artículo derivado del marco conceptual en:

http://hades.funsalud.org.mx/cerberus/thesis.html
y
http://portal-pocket.dgsca.unam.mx en la comunidad denominada "seguridad y *virus*".[47]

También el apartado denominado "Virtualia" del periódico "El Universal" se ha comprometido en colocar el mismo artículo en su publicación.

[47] Ambos enlaces aún siguen vigentes al día 24 de noviembre del 2000.

5.2.B. Ofertamiento personal.

Ofertamiento personal para presentar conferencias en eventos relacionados con la seguridad informática.

Día 18 de mayo del 2000 el autor impartió la conferencia: Factores de riesgo en centros de cómputo en el colegio "Partenón".

Día 11 y 12 de noviembre del 2000 el autor impartió la conferencia "Seguridad en códigos distribuibles en internet" para la empresa DDMESIS.

VideoConferencia de la FCA. Efectuada el día 15 de julio. La conferencia se llamó "Informática una herramienta para la administración" donde se mencionó parte del esfuerzo realizado por el autor por dar a conocer el primer intento por erguir en el campo de la seguridad computacional en el ámbito académico.

5.2.C. Inclusión en la currícula académica.

Inclusión en la currícula académica, pudiendo ser:

- Temática en la materia "Administración de centros de cómputo" impartida en noveno semestre de la licenciatura en informática.
- Temática en la materia "Auditoria informática" impartida en décimo semestre de la licenciatura en informática.
- Integral como materia optativa pudiéndose denominar "Seguridad en computadoras y redes de computadoras" pudiéndose impartir en los semestres terminales de la licenciatura en informática.
- Integral dándole un enfoque meramente informativo en vez de un enfoque matemático tal y como se ha venido dando con la materia "criptografía y seguridad" impartida en 10°. Semestre en la licenciatura en informática. De hecho un apartado de la materia propuesta estaría enfocado a la criptografía.

En caso de tratarse de una materia temática obligatoria el temario que se sugiere puede tener la estructura siguiente:

1. Seguridad en cómputo.

1.1) Definiciones de seguridad en cómputo.
1.2) ¿Qué recursos intentamos proteger ?
1.3) ¿Contra qué?
1.4) Resumen extendido de una clasificación de seguridad en centros de cómputo.

2. *Ataques* a computadoras y a redes de computadoras.

2.1) Atacantes y sus objetivos.
2.2) Accesos.
2.3) Resultados.
2.4) Herramientas.
   a) Comandos de usuario.
   b) Scripts o programas.
   c) Agentes autónomos.
   d) Toolkits.
   e) Herramientas distribuidas.
   f) Data tap.

5.2.D. Divulgación para crear cursos en empresas dedicadas a la educación.

Cualquier comentario, duda, sugerencia y/o invitación a impartir algún curso, diplomado o seminario es bienvenida a la dirección de correo electrónico cerberus@hades.funsalud.org.mx donde se puede trabajar en algún temario particular.

VI. CONCLUSIONES.

6.1 Conclusiones.

Este trabajo generó dos productos útiles en cuestión de seguridad computacional. En primer lugar se propuso una taxonomía de ataques a computadoras y a redes de computadoras con la finalidad de clasificar los incidentes de seguridad a los que están expuestos esos equipos; y en segundo lugar sirvió para demostrar que el realizar un análisis de riesgos conlleva variadas ventajas que se deberían tomadar en cuenta por todas aquellas personas que utilizan a diario computadoras.

Entre las conclusiones derivadas de este trabajo se encuentran las siguientes:

- Se puede decir que una taxonomía es una aproximación a la realidad que es utilizada para tener un mejor entendimiento sobre un campo de estudio. Una taxonomía puede clasificar categorías con las siguientes características:

  1) Mutuamente excluyente.- La clasificación de una entidad en una categoría la excluye de todas las demás características.
  2) Exhaustiva.- Tomando todas las categorías, se incluyen todas las posibilidades.
  3) No ambigua.- Para clasificar una entidad se debe percibir que la asignación es clara y precisa. Una clasificación no puede ser incierta.
  4) Repetible.- Las aplicaciones que se repitan deben caer en la misma clasificación sin importar quién es la persona que esta llevando a cabo la clasificación.
  5) Aceptada.- Lógica e intuitiva.
  6) Útil.- Reutilizable cada vez que se quiera clasificar una entidad de la misma naturaleza.

- Una simple y popular taxonomía de ataques a computadoras y a redes de computadoras es una lista sencilla que solamente define términos. Hay algunas variaciones a este tipo de clasificación y provocan listas de categorías. Con este tipo de clasificación se han encontrado algunos problemas que limitan este tipo de referencias, tales como:

  1) Los términos no son mutuamente excluyentes.
  2) Una lista exhaustiva comienza a volverse difícil de utilizar y muy larga.
  3) Las definiciones de términos individuales se toman muy difíciles.
  4) No existe una estructura de categorías.

- Un método de categorización alternativa corresponde a la estructura de las categorías en una matriz. Sin embargo, se puede volver ambigua cuando se intentan clasificar una lista enorme de tipos de ataques a equipos de cómputo.

- La taxonomía que se desarrolla en este trabajo de investigación no intenta enumerar todos los incidentes de seguridad. Tampoco pensar que se desea contar con un diccionario que indique todos los métodos de ataques. La taxonomía mostrada en este

trabajo intenta mostrar una taxonomía en centros de computo pero teniendo como base una clasificación simple por categorías basadas en un proceso.

- La taxonomía final presentada fue desarrollada desde una definición de seguridad en cómputo, se enriqueció de una crítica hacia las taxonomías actuales y se realizó desde un punto de vista operacional, desde todo un proceso.

- Desde este punto de vista, un atacante en una computadora o en una red de computadoras intenta alcanzar por determinada motivación sus objetivos. Este intento se establece a través de una secuencia operacional en donde se encuentran involucradas herramientas, mecanismos de acceso, y resultados que conectan a esos atacantes contra sus objetivos.

- Con una taxonomía como esta cada empresa podría comenzar a elaborar análisis de riesgos con una visión más objetiva.

- Los análisis de riesgos dentro de las organizaciones son realizados por distintos tipos de personas, con o sin conocimientos de seguridad en cómputo. El porcentaje de personas que realizan análisis de riesgos sin conocimientos es mucho mayor que el porcentaje de personas preparadas que lo realizan.

- El realizar un análisis de riesgos con una base de conocimientos real permite determinar algunas necesidades no detectadas en la empresa, cuantificar los riesgos a los cuales están sujetos los activos y estimar la probabilidad de ocurrencia de cada riesgo latente.

- Además, si se realizan análisis de riesgos en la información en centros de cómputo, se pueden revisar y redefinir los controles de seguridad ya existentes y hacer una correcta distribución de recursos humanos, financieros y/o materiales de las actividades del centro.

VII. GLOSARIO Y ABREVIATURAS.

7.1. Glosario de términos.

Análisis de riesgos.- El proceso de estudiar los activos del procesamiento de información y sus vulnerabilidades para determinar una pérdida esperada de eventos dañinos, basada en la probabilidad de ocurrencia.

Ataque.- Acción que compromete la seguridad de la información.

Autenticación.- Servicio que involucra un requerimiento de identidad o identificación corroborable y distingue entre la autenticación de las partes que se comunican entre sí y la autenticación del origen de los datos.

Bug.- Un error en un código o en la lógica de un programa que causa que un programa funcione de manera incorrecta o produzca resultados incorrectos.

Caballo de Troya.- Programa que aparentemente es válido y útil, pero contiene instrucciones ocultas cuya ejecución causa consecuencias no conocidas por el usuario. Sólo programadores experimentados pueden construir caballos de Troya. Una vez infiltrado en un sistema es muy difícil de detectar.

Ciudad de México.- Zona comprendida por el Distrito Federal y los 17 municipios conurbados del Estado de México.

Ciudad Universitaria.- Zona sur de la ciudad de México donde se encuentra el campus de la Universidad Nacional Autónoma de México en el Distrito Federal. Se encuentra delimitada por varias avenidas importantes incluyendo avenida insurgentes, avenida de la IMAN y avenida universidad.

Cifrado.- Texto no legible que resulta de aplicar una (o varias llaves) a un texto legible (muchas veces conocido como texto en claro o texto legible).

Confidencialidad.- Proporciona a los datos protección contra lectura o divulgación no autorizada. Este servicio oculta o transforma los datos de tal manera que solo las partes autorizadas puedan enterarse de su contenido.

Control de acceso.- Servicio que proporciona protección a los recursos del sistema contra acceso y uso no autorizado. Este servicio esta íntimamente relacionado al de autenticación debido a que un usuario o proceso debe ser autenticado antes de tener acceso a cualquier recurso del sistema.

FAT.- El sistema utilizado por MSDOS para organizar y administrar los archivos. La FAT (File Allocation Table) es una estructura de datos que MSDOS crea en el disco cuando éste es formateado.

Firewall.- Un sistema basado en hardware o software que protege al sistema interno o a una red interna del ambiente exterior (por ejemplo, internet) o protege a una parte de una red de otra. Básicamente un firewall monitorea todo el tráfico (véase tráfico) permitiendo pasar sólo algunos paquetes de datos (los que tienen permitido hacerlo por políticas de seguridad) y bloqueando el resto.

Hacker.- Persona que intenta tener acceso no autorizado a computadoras mediante el uso de computadoras. Generalmente lo hace por el reto intelectual y el desafío tecnológico que esto implica, pero casi nunca con fines perjudiciales.

Integridad.- Servicio que protege a los datos contra modificaciones, alteraciones, borrado, inserciones y de todo tipo de acción que atente contra su integridad.

Intruso.- Un usuario no autorizado o un programa no autorizado generalmente con una intención maliciosa dentro de una computadora o dentro de una red de computadoras.

IP spoofing.- Método de spoofing (véase spoofing) en el cual un atacante no coloca las direcciones IP en los paquetes de datos enviados a internet para que parezcan que provienen de un sitio dentro de la red en el cual se asume como confiable.

Llave(s).- Cadena de caracteres que al aplicarse a un mensaje en lenguaje natural junto con un algoritmo de transformación produce un mensaje cifrado o codificado.

No repudio. El no repudio proporciona protección contra el repudio. Véase Repudio.

Orange Book.- Department of Defense Trusted Computer System Evaluation Criteria, DOD 5200.28-STD. Un estándar publicado por el gobierno de los Estados Unidos para clasificar la seguridad de los sistemas de cómputo en cuatro divisiones jerárquicas –A, B, C y D – para satisfacer el nivel de confianza requerido por dicho gobierno para una aplicación particular.

Privacidad. Sinónimo de confidencialidad. Véase Confidencialidad.

Repudio.- Posibilidad de que alguna de las partes involucradas en una comunicación nieguen ya sea haber enviado o bien nieguen haber recibido un mensaje o haber sido el destinatario de cierta acción

Seguridad física.- Conjunto de lineamientos y procedimientos cuyo objetivo es evitar o disminuir la exposición a riesgos, ya sean internos o externos, en las instalaciones físicas del centro de cómputo.

Servicio de seguridad.- Funcionalidad específica que forma parte de la seguridad de un sistema y de su transferencia de información.

Shell.- Una pieza de software, usualmente un programa separado, que proporciona comunicación directa entre un usuario y un sistema operativo. Ejemplos de shells son el Macintosh Finder y la interface de comandos de MSDOS. En el caso de Unix (véase unix) los shells más utilizados son el Bourne shell, C shell y korn shell.

Sitc.- Lugar o "sitio" donde esta instalado, o puede ser instalado, cierto equipo de cómputo.

Spoofing.- Pasar como un usuario autorizado, usualmente es un intento para ganar acceso a un sistema.

Taxonomía.- Una manera inteligente de clasificar las cosas.

Tráfico.- El flujo de mensajes a través de una red.

Unix. – Sistema operativo multiusuarios y multitareas originalmente desarrollado por Ken Thompson y Dennis Ritchie en los Laboratorios ATT en 1969 para usarse en minicomputadoras. UNIX es considerado actualmente como uno de los más poderosos sistemas operativos existentes. Esta hecho en lenguaje C.

Virus.- Programa que modifica a otros programas o a archivos. Un virus generalmente se propaga replicándose a sí mismo y contagiando a otros programas. En algunos casos, un evento predeterminado activa al virus para llevar a cabo su propósito modificador o destructivo.

Vulnerabilidad.- Susceptibilidad de un sistema a una amenaza de ataque específico o evento dañino.

6.2. Abreviaturas y acrónimos.

BBS.- Bulletin Board System (sistema electrónico de mensajes que generalmente corre en microcomputadoras).

D.C.A.A.- Dirección de Cómputo para la Administración Académica.

D.G.S.C.A.- Siglas de la Dirección General de Servicios de Cómputo Académico.

IEC.- International Electrotechnical Committee (Comité Electrotécnico Internacional).

ISO.- International Organization for Standarization (Organización Internacional para la Estandarización).

ITU-T.- International Telecommunication Union (Unión Internacional de las Telecomunicaciones) Telecommunication Standarization Sector (Sector de Estandarización de las Telecomunicaciones).

JTC-1.- Joint Technical Committee 1 (Comité Técnico Conjunto 1).

LGSN.- Protocolos criptográficos de la familia LGSN. Siglas de sus autores: Lomas, Gong, Saltzer, Needham).

OSI.- Modelo de Referencia OSI. OSI (Open Systems Interconection – Interconexión de sistemas abiertos).

RDBMS.- Relational DataBase Management System.