UNIVERSIDAD NACIONAL AUTÓNOMA DE NICARAGUA

UNAN-MANAGUA

RECINTO UNIVERSITARIO RUBÉN DARÍO

FACULTAD DE CIENCIAS E INGENIERÍAS

SEMINARIO DE GRADUACIÓN

TEMA:

Computación Forense

SUBTEMA:

Seguridad informática en el centro de cómputo del Hospital Militar Escuela “Dr. Alejandro Dávila Bolaños”.

TUTOR:

Lic. Juan de Dios Bonilla Anduray

PRESENTAN:

Br. María Isabel Medina Morales

Br. Maybel Tatiana Martínez Ojeda

JUNIO, 2011

DEDICATORIA

El presente trabajo lo dedico en primer lugar a **DIOS**, por haberme dado la vida y la capacidad de terminar mis estudios universitarios, particularmente la realización de este trabajo. A mi madre **Rosario Ojeda Borge** por haberme dado su apoyo y comprensión incondicional siempre que lo necesité.

Maybel Tatiana Martínez Ojeda.

El presente trabajo lo dedico a **DIOS**, por haberme dado sabiduría, entendimiento y perseverancia para terminar este trabajo con éxito. A mis padres **Sara Morales** y **Pedro Medina** por apoyarme y animarme a seguir adelante.

María Isabel Medina Morales.

AGRADECIMIENTO

Agradecemos en primer lugar a **DIOS** que nos ha dado la vida, la inteligencia, sabiduría y fortaleza para emprender este trabajo y concluirlo exitosamente.

A nuestro tutor **Juan de Dios Bonilla Anduray** por habernos guiado durante toda la realización del trabajo.

A nuestros padres y amigos que nos han alentado y apoyado durante todo el transcurso de esta carrera.

ÍNDICE

I.RESUMEN

El presente trabajo pretende desarrollar un tema relacionado a la computación forense, este es: Seguridad informática en el centro de cómputo del Hospital Militar Escuela “Dr. Alejandro Dávila Bolaños”.

La seguridad informática es un componente muy importante en el campo de la computación, debido a que esta área es la principal responsable de proteger tanto el hardware como el software de una institución, pero muchas veces es considerado como algo que puede planificarse después, no obstante, es suficiente una única brecha en la seguridad para provocar daños irreparables en la institución.

El documento contiene un marco conceptual de los aspectos más importantes relacionados al desarrollo de la investigación, sin embargo, considerando la continua evolución tecnológica, la actualización sobre el tema debe ser de forma persistente.

Se incluye en el documento, el diseño de un plan de seguridad para el centro de cómputo, que plantea acciones para fortalecer la seguridad informática y corregir posibles vulnerabilidades.

II. INTRODUCCIÓN

Toda organización debe estar a la vanguardia de los procesos de cambio. Donde disponer de información continua, confiable e integra constituye una ventaja fundamental, sin embargo, con el avance de la tecnología informática surgen riesgos que pueden afectar severamente la continuidad de la organización. En este contexto aparece la seguridad informática cuyo objetivo es reducir las oportunidades de que un sistema sea comprometido o al menos disminuir los daños provocados a raíz de un ataque.

La seguridad informática se obtiene por medio de: políticas de seguridad, herramientas de seguridad (firewall, IDS), medidas de control, planes de contingencia y auditorias; el incumplimiento de estos elementos provoca la inseguridad informática, la cual es responsable de que un sistema sea accedido por intrusos y que la información sea alterada o sustraída. Por tanto garantizar la seguridad de la información es un objetivo inaplazable primordialmente para el área informática de cualquier organización.

Actualmente el centro de cómputo del Hospital Militar "ADB" no cuenta con un plan de seguridad informática que ayude al fortalecimiento de dicha seguridad en esta institución.

Por lo tanto el presente trabajo tiene como finalidad diseñar un plan de seguridad informático basado en la norma ISO 27001 para el centro de cómputo del Hospital Militar "ADB".

III. PLANTEAMIENTO DEL PROBLEMA

El crecimiento de la tecnología en Nicaragua en los últimos años ha tomado gran fuerza logrando grandes beneficios económicos a las empresas e instituciones del país.

Sin embargo, junto con este avance tecnológico han surgido problemas relacionados a la seguridad informática que es un campo muy nuevo y por ello de poco desarrollo en las empresas nicaragüenses.

Actualmente las dificultades más relevantes que se presentan son:

1. Algunas instituciones del país se limitan a utilizar pocos mecanismos de seguridad.
2. Es muy común la inexistencia de políticas de seguridad escritas y aunque estas existan el personal informático no esta plenamente consciente de la importancia de ejecutarlas.
3. El presupuesto económico consignado a las áreas de informática no es suficiente para cubrir todas las necesidades que se presentan.

Generalmente estas dificultades son más comunes en las instituciones públicas y las microempresas que en las empresas privadas del país, esto se debe a que las empresas privadas disponen de un mayor capital económico.

IV.JUSTIFICACIÓN

El presente trabajo es una valoración de la seguridad informática en el centro de cómputo del Hospital Militar “ADB”.

Con el resultado de esta valoración el jefe de informática y demás personal involucrado, podrán conocer las debilidades que tiene el centro de cómputo y las acciones que se deben establecer para mejorarlas, cada una de estas acciones están contempladas por la norma ISO 27001.

Igualmente se intenta ayudar a sensibilizar al personal que labora en el centro de cómputo del Hospital Militar “ADB” sobre lo indispensable que es el cumplimiento de las políticas y medidas de seguridad.

V. OBJETIVOS

5.1. Objetivo General

- Valorar la seguridad informática del centro de cómputo del Hospital Militar Alejandro Dávila Bolaños.

5.2. Objetivos Específicos

- Colaborar en la concienciación de las personas que laboran en el departamento de informática del Hospital Militar Alejandro Dávila Bolaños, sobre la importancia y el alcance que tiene la Seguridad Informática.

- Identificar puntos vulnerables que puedan afectar la seguridad informática en el centro de cómputo.

- Elaborar un plan de seguridad informática, basado en los controles A.5, A.7, A.9, A.10, A.11 Y A.12 que contiene la norma ISO 27001.

VI.DESARROLLO

6.1. Marco teórico

6 .1.1. Seguridad informática

6.1.1.1. Definición

La Seguridad es Calidad de seguro, donde Seguro es Libre y exento de Peligro, por lo que podríamos concluir que Seguridad Informática es "la calidad de un sistema informático exento de peligro"[1]. Sin embargo, esta a pesar de que puede ser una definición valida, no es una definición aceptable ya que al abordar el tema de Seguridad Informática, se debe tener muy en claro que no existe una seguridad en términos absolutos ya que siempre es posible quebrantar la seguridad de un sistema o de una red, no obstante, gracias a los mecanismos y planes de contingencia comprendidos por la seguridad informática es posible controlar rápidamente una situación de riesgo después de un ataque.

Una definición más acertada sería la siguiente: Un conjunto de métodos y herramientas destinados a proteger la información y por ende, los sistemas informáticos ante cualquier amenaza[2].

La seguridad informática es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta (incluyendo la información). Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información.

[1]Wikibooks. (n.d).Seguridad informática. Obtenida el 14 de septiembre de 2010, de http://es.wikibooks.org/wiki/Seguridad_inform%C3A1tica/Definici%C3%B3n.

[2]Wikipedia. (n.d).Seguridad informática. Obtenida el 14 de septiembre de 2010, de http://es.wikipedia.org/wiki/seguridad_ inform%C3%A1tica.

La seguridad de la información es una sub área de la seguridad informática que se enfoca exclusivamente en la protección de la información, lo que comprende software, bases de datos, archivos y todo lo que la organización valore (activo) y signifique un riesgo si ésta sufre algún daño o alteración.

Al tratar el asunto de la seguridad informática, se está considerando que se encuentran en riesgo tres elementos:

a) Los datos: información guardada en las computadoras.

Los datos tienen tres características a proteger:

- Confidencialidad
- Integridad
- Disponibilidad

b) Los recursos: el equipamiento en sí mismo

c) La reputación

6.1.1.2. Objetivos de la seguridad informática

El principal objetivo de la seguridad informática es proteger los activos informáticos de cualquier empresa o institución entre los que se encuentran:

- La información

  Este activo se ha convertido en uno de los elementos más importantes y valiosos dentro de una organización. La seguridad informática debe ser administrada según los criterios establecidos por los administradores y supervisores, evitando que usuarios externos y no autorizados puedan acceder a ella sin autorización. De lo contrario la organización corre el riesgo de que la información sea utilizada maliciosamente para obtener ventajas de ella o que sea manipulada, ocasionando lecturas erradas o incompletas de la misma. Otra función de la seguridad informática en esta área es la de asegurar el acceso a la información en el momento oportuno, incluyendo respaldos de la misma en caso de que esta sufra daños o pérdida producto de accidentes, atentados o desastres.

- La infraestructura computacional

  La función de la seguridad informática en esta área es velar que los equipos funcionen adecuadamente y prever en caso de que ocurra alguna falla planes de robos, incendios, boicot, desastres naturales, fallas en el suministro eléctrico y cualquier otro factor que atente contra la infraestructura informática.

- Los usuarios

  Son las personas que utilizan la estructura tecnológica, la seguridad informática debe establecer normas que minimicen los riesgos a la información o infraestructura informática. Estas normas incluyen horarios de funcionamiento, restricciones a ciertos lugares, autorizaciones, denegaciones, perfiles de usuario, planes de emergencia, protocolos y todo lo necesario que permita un buen nivel de seguridad informática minimizando el impacto en el desempeño de los funcionarios y de la organización en general.

6.1.1.3. Amenazas a la seguridad informática

Las amenazas son circunstancias que pueden afectar a los datos, estas amenazas son a menudo imprevisibles o inevitables, de modo que la única protección posible es el continuo respaldo de la información y la descentralización mediante estructura de redes en el caso de las comunicaciones. [3]

Las amenazas pueden ser direccionadas a:

- Servidores
- Red
- Aplicaciones web

[3] Wikipedia. (n.d).Seguridad informática. Obtenida el 14 de septiembre de 2010, de http://es.wikipedia.org/wiki/seguridad_ inform%C3%A1tica.

El hecho de conectar una red a un entorno externo nos da la posibilidad de que algún atacante pueda entrar en ella, con esto, se puede hacer robo de información o alterar el funcionamiento de la red. Sin embargo el hecho de que la red no sea conectada a un entorno externo no nos garantiza la seguridad de la misma. De acuerdo con el Computer Security Institute (CSI) de San Francisco aproximadamente entre 60 y 80 por ciento de los incidentes de red son causados desde adentro de la misma. Basado en esto podemos decir que existen 2 tipos de amenazas:

- Amenazas internas: Generalmente estas amenazas pueden ser más serias que las externas por varias razones como son:
  - Los usuarios conocen la red y saben cómo es su funcionamiento.
  - Los Firewalls son mecanismos no efectivos en amenazas internas.
  - Tienen un nivel de acceso a la red por su trabajo.

- Amenazas externas: Son aquellas amenazas que se originan de afuera de la red. Al no tener información certera de la red, un atacante tiene que realizar ciertos pasos para poder conocer qué es lo que hay en ella y buscar la manera de atacarla. La ventaja que se tiene en este caso es que el administrador de la red puede prevenir una buena parte de los ataques externos.

6.1.1.4. Análisis de riesgo informático

El activo más importante que se posee es la información y por lo tanto, deben existir técnicas que la aseguren, más allá de la seguridad física que se establezca sobre los equipos en los cuales se almacena. Estas técnicas las brinda la seguridad lógica que consiste en la aplicación de barreras y procedimientos que resguardan el acceso a los datos y sólo permiten acceder a ellos a las personas autorizadas para hacerlo. [4]

[4] Chávez, A. (2009).Seguridad informática. Obtenida el 14 de septiembre de 2010, de http://www.biblioteca.clacso.edu.ar/recursos/seguridad-informatica.pdf.

Una de las actividades iníciales para gestionar la seguridad informática dentro de las organizaciones es el análisis de riesgos, para lo cual, se debe realizar un modelado de amenazas, se trata de una actividad de carácter recurrente, pero también se deben tomar en cuenta otros puntos a seguir:

1. Identificación de los activos de la organización.
2. Identificar las amenazas de cada uno de los activos listados.
3. Conocer las prácticas actuales de seguridad.
4. Identificar las vulnerabilidades de la organización.
5. Identificar los requerimientos de seguridad de la información.
6. Identificación de las vulnerabilidades dentro de la infraestructura tecnológica.
7. Detección de los componentes claves.
8. Desarrollar planes y estrategias de seguridad que contengan los siguientes puntos:

    - Riesgo para los activos críticos
    - Medidas de riesgos
    - Estrategias de protección
    - Planes para reducir los riesgos.[5]

[5]Obtenido de Wikipedia. (n.d).Seguridad informática. Obtenida el 14 de septiembre de 2010, de http://es.wikipedia.org/wiki/seguridad_ inform%C3%A1tica. y Chávez, A. (2009).Seguridad informática. Obtenida el 14 de septiembre de 2010, de http://www.biblioteca.clacso.edu.ar/recursos/seguridad-informatica.pdf.

6.1.1.5. Inseguridad Informática

6.1.1.5.1. Inseguridad centralizada

Durante los años 60 y 70 la computación centralizada era la realidad evidente de los centros de procesamiento de datos. Los grandes computadores centrales eran los que estaban en el primer nivel del uso informático de las organizaciones. Este tipo de computación era la norma que apoyaba los diferentes procesos de la organización, los cuales eran operados por personal especializado para esas labores. Es importante anotar que no todo el mundo tenía acceso a estas máquinas. En este sentido, la seguridad informática alrededor de este escenario, más que concentrarse en el descubrimiento de la inseguridad de los programas, estaba orientada a la seguridad física de los equipos y el buen procesamiento de la información. Una falla en el control de la información, o en la integridad de la misma, generaba una alta desconfianza en los informes y sus cifras.

La computación centralizada y basada en un gran mainframe estaba dominada por las recomendaciones de los proveedores y no seguirlas era ir en contra del buen funcionamiento de las máquinas. En este mismo sentido, la seguridad de la información se concentraba en el acceso y el control de las máquinas, en el ingreso al sitio donde se encuentran éstas, y en la habilidad y el entrenamiento de las personas encargadas de operarlas.

En cuanto a la seguridad y el control, los años 60 y 70 se caracterizaron por un énfasis marcado en el control de acceso, la segregación de funciones y el debido registro de las operaciones y transacciones. Los mecanismos de seguridad propios de la época eran registros de auditoría que, si bien existían y eran frecuentemente consultados, no tenían mayores protecciones, dado que el personal que tenía acceso a ellos eran profesionales con alto nivel de confianza y con perfiles especiales, claramente registrados e identificados. [6]

[6] Cano, J. (2009).Computación forense, Descubriendo los rastros informáticos. México: Alfaomega Grupo Editor, S.A de C.V.

Esta es la época de aplicación de modelos de seguridad, como Bell-Lapadula y Biba Model, modelos que hacían hincapié en la confidencialidad y el acceso a la información.

6.1.1.5.2. Inseguridad descentralizada

Durante los años 80 se pasaba de una realidad centralizada y cerrada, a una descentralizada y abierta. Se concluye la época de los mainframes y se abre la puerta al concepto de las infraestructuras cliente/servidor. En este modelo de interacción existen máquinas que solicitan servicios y otras que los ofrecen. El énfasis se concentra en el tráfico de información a través de la red, y el uso de puertos de conexión, los cuales están asociados con los servicios que se prestan.

Este cambio abre la puerta a un nuevo tipo de inseguridad, a unas nuevas relaciones que van más allá del servidor centralizado y, por tanto, requiere repensar la gestión de la seguridad de la información. Con la llegada de una computación más abierta y con más oportunidades, se inicia la carrera para desarrollar mecanismos de seguridad de información, particularmente orientada a las redes: firewalls, sistemas de detección de intrusos (IDS), criptografía, proxies, entre otros, los cuales establecen una nueva responsabilidad para el área de tecnologías de información.

Los nuevos mecanismos de seguridad que se presentan recogen las prácticas de los años 70 y desarrollan nuevas funcionalidades para disminuir los impactos de la inseguridad propia de los protocolos asociados con TCP/IP. Ahora, en el mundo c/s, el director de tecnología no solamente es responsable porque la infraestructura funcione de acuerdo con lo requerido, sino que debe hacerlo con mayor confiabilidad, disponibilidad, trazabilidad e integridad. [7]

[7] Cano, J. (2009).Computación forense, Descubriendo los rastros informáticos. México: Alfaomega Grupo Editor, S.A de C.V.

Este requerimiento se hace en medio de una nueva tendencia de ataques y de incidentes que llevan a las organizaciones a fallas importantes de los sistemas y a perdidas de continuidad, ya no ocasionadas por una caída del servidor central, sino por el acceso no autorizado, una negación de servicios, una suplantación de direcciones IP, envenenamiento de caché del DNS (Domain Name Services), monitoreo no autorizado de conexiones, suplantación de direccione MAC, asalto de sesiones TCP, ente otros.

Esta nueva realidad desarrolla y propulsa una dinámica de la seguridad de la información, no solamente motivada por los ataques sino por las posibilidades que se abren al explorar los protocolos que soporta la suite de protocolos TCP/IP. Las aplicaciones cliente/servidor ofrecen toda una gama de nuevas posibilidades para usar la capacidad de cómputo de las máquinas, y abrir la interacción de las mismas a los usuarios de toda la organización.

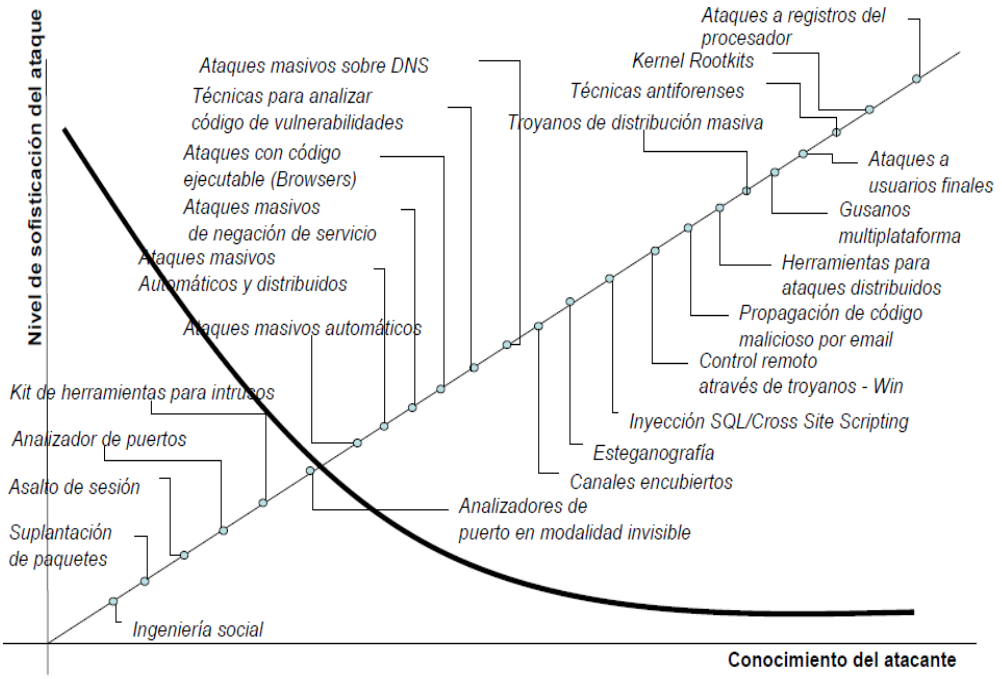
6.1.1.5.3. Evolución de la inseguridad informática

Este es el momento cuando nos movemos hacia la utilización masiva de la Web, cabe preguntar: ¿Qué vendrá luego? La respuesta es: con toda seguridad, lo mejor y de mayor versatilidad; algo que nos permitirá ver mayores integraciones entre lo expuesto en la red, con los sistemas inalámbricos las estrategias corporativas.

La convergencia tecnológica nos llevará a un escenario de tecnologías híbridas de uso cotidiano, donde mayores relaciones y productos estarán en juego y el usuario será el mayor beneficiado sin embargo, siempre estará la ventana de exposición abierta a nuevas posibilidades y mutaciones de las vulnerabilidades informáticas, la generación de plagas electrónicas más adaptables y polimórficas, un escenario en donde la inseguridad sabrá mostrar por qué ella es parte inherente del desarrollo tecnológico de las organizaciones y de las naciones . [8]

[8] Cano, J. (2009).Computación forense, Descubriendo los rastros informáticos. México: Alfaomega Grupo Editor, S.A de C.V.

Evolución de los ataques de seguridad



Considerando las diferentes evoluciones tecnológicas revisadas, así como la transformación de la seguridad de la información, es preciso que los investigadores forenses en informática profundicen cada vez más en las posibilidades que ofrece la tecnología y sus efectos de borde, así como las formas como los intrusos pueden aprovecharse de estas posibilidades, bien sea para evadir una investigación o para desviarla; de conformidad con la computación forense, la convergencia tecnológica es un riesgo que se advierte, pues en los puntos de contactos entre tecnologías frecuentemente existen pocos puntos de rastro vinculante (para realizar la construcción de los hechos) , lo cual limita el accionar de los investigadores en este sentido. [9]

[9] Cano, J. (2009).Computación forense, Descubriendo los rastros informáticos. México: Alfaomega Grupo Editor, S.A de C.V.

6.1.1.5.4. Dualismo de la Seguridad Informática

El dualismo, ha sido factor clave para el desarrollo de muchos conceptos que hoy en día son fundamentales para el avance de la tecnología y la seguridad informática, pero no es la única estrategia para abordar los fenómenos de nuestra realidad. En la perspectiva del dualismo un sistema es seguro o inseguro, lo que implica reconocer y profundizar en un lado de línea de pensamiento. Es decir, o aplicamos técnicas de seguridad informática para reducir los riesgos e implementar controles, ó vemos como podemos saber que tantas vulnerabilidades tenemos que nos hacen inseguros, para tomar medidas correctivas.

En este sentido, se presenta la estrategia de la dualidad, como una manera complementaria de explorar los hechos mismos en el mundo, para reconocer las causas y los efectos en su contexto, sin negar la posibilidad de considerar que uno surge a partir del otro, es decir, reconocer que la seguridad informática surge a partir de considerar la inseguridad informática y viceversa.

En múltiples investigaciones realizadas se considera el tema de la seguridad informática como una disciplina del conocimiento donde se busca cerrar la brecha de los eventos inesperados que puedan comprometer los activos de una organización y así contar con estrategias para avanzar ante cualquier eventualidad.

Se considera ahora el estudio de la inseguridad informática, como una disciplina dual donde los académicos y practicantes de la industria buscan las maneras detalladas para que ocurran eventos inesperados, establecen las condiciones extremas de funcionamiento de los dispositivos o estrategias, todo con el fin de hacer caminar en condiciones límite la operación de la organización y sus negocios.[10]

[10] Cano, J. (2004).Inseguridad informática: un concepto dual en seguridad informática. Obtenida el 12 de marzo de 2011, de http://www.virusprot.com/art47.html

¿Cómo funciona el sistema?

¿Cómo no funciona el sistema?

¿Cómo reacciona ante una falla?

¿Cómo hacerlo fallar?

Por tanto, la inseguridad informática como disciplina dual en el estudio de la seguridad informática, establece un paradigma complementario (es decir dual a la seguridad informática) que comprende las propiedades emergentes de los sistemas (analizados) bajo condiciones y realidades extremas, las cuales no son viables en una estrategia de protección causal (dualismo) sugerida por la seguridad informática actual. En este sentido, se quiere plantear la necesidad de revisar la manera en que se aborda el tema de la protección de los activos de una organización, no solamente establecer las causas y los efectos, sino comprender las relaciones entre los objetos revisados y considerar las reacciones mismas de entre estas que pueden sugerir efectos no predecibles en los modelos causales.

Se requiere que el equipo de pruebas trabaje sobre la descripción del comportamiento del producto o sistema, se requiere que el producto o sistema sea ejecutado en un ambiente real o simulado, Se requiere que la funcionalidad del producto o sistema sea explorada de una manera metódica y que los resultados de las pruebas bien sean positivos o negativos, puedan ser analizados en contexto y así ofrecer un concepto formal del mismo; en este contexto, las relaciones causales deben ser determinadas y concretadas de tal manera que sea posible detallar y sustentar los posibles estados exhibidos por el sistema al ser sometido a las pruebas de comportamiento sugeridas dentro del dominio de la definición del producto mismo. Esta estrategia si bien aporta elementos detallados sobre el sistema y su funcionamiento futuro, nos ofrece pocas luces sobre comportamientos inesperados y condiciones extremas de operación, dado que no se abre la posibilidad a una lógica de la inseguridad informática como reflexión dual del ejercicio. [11]

[11] Cano, J. (2004).Inseguridad informática: un concepto dual en seguridad informática. Obtenida el 12 de marzo de 2011, de http://www.virusprot.com/art47.html

Al revisar la inseguridad informática como estrategia de pensamiento estratégico se reconoce que un sistema es tan seguro como su falla de seguridad más reciente, que cuando ocurre o se manifiesta un problema de seguridad las personas se vuelven más experimentadas y saben qué hacer, que los sistemas mal diseñados (pensamiento natural en seguridad informática) no están preparados para fallar (pensamiento dual en inseguridad informática).

La inseguridad informática como pensamiento dual en seguridad informática descubre que las relaciones entre los elementos del sistema son capaces de producir efectos positivos y negativos, los cuales son capaces de comprometer su supervivencia. En este sentido, comprender la inseguridad informática como el dual de la seguridad informática, en el contexto organizacional, representada esta última en sus participantes, sus procesos y tecnología, nos permite revisar las propiedades emergentes de la seguridad informática en un escenario con múltiples variables, repensar la seguridad misma mas allá de una directriz de la corporación, como una mente pensante que aprende y evoluciona en su hacer.

El concepto de la organización como una mente pensante y actuante, con un pensamiento complementario (dual) nos sugiere que la seguridad informática, como una distinción más de la organización, representa una dinámica de acción que podríamos recrear considerando los elementos de la mente segura, una mente segura consiste en la revisión y práctica de virtudes y reglas de seguridad con el fin de tomar decisiones claras, consistentes y efectivas. Complementario a esta propuesta, la existencia de la mente insegura, como realidad presente de la organización, es un punto de análisis adicional que se considera, no solo para dar sentido a la práctica de las virtudes y reglas de seguridad, sino para mantener la perspectiva de la incertidumbre inherente al proceso de la seguridad informática. [12]

[12] Cano, J. (2004).Inseguridad informática: un concepto dual en seguridad informática. Obtenida el 12 de marzo de 2011, de http://www.virusprot.com/art47.html

La mente insegura como dual de la mente segura, puede sugerir elementos de análisis de situaciones extremas en las organizaciones que lleven no solamente a considerar las vulnerabilidades y riesgos de las información de los procesos de la empresa, sino repensar los procesos mismos para hacerlos más confiables, en la medida que se consideren las diferentes perspectivas de la seguridad implícitas en cada uno de los participantes de los mismos. La mente insegura es una posibilidad de caminar y entender la senda del análisis de riesgos como un modelo de hacking consistente de reconocimiento del sistema objetivo, manipulación y compromiso del objetivo, apalancamiento del ataque y conquista de nuevos objetivos.

Mientras la seguridad informática es un concepto subjetivo es decir propio al sujeto, la inseguridad informática es objetiva, es decir propia al objeto. No es posible evitar la inseguridad informática pues es una propiedad inherente a los objetos. Por tal motivo, se hace necesario explorar en profundidad dicha propiedad, pues mientras más se comprenda la realidad de la inseguridad, con mejores ojos podremos comprender la seguridad informática de las organizaciones.

Considerar la inseguridad informática como parte del ejercicio de seguridad informática de las organizaciones, sugiere la capacidad de las organizaciones para cuestionarse sobre la situación real del balance entre seguridad, facilidad de uso y funcionalidad no para lograr mayores niveles de confiabilidad y aseguramiento de sus arquitecturas, sino para evaluar el nivel de dificultad requerido por los atacantes para ingresar y vulnerar los medios de protección. Con un pensamiento de este nivel, las organizaciones no buscarán solamente incrementar la confianza de sus clientes, sino comprender que la seguridad no es un problema de tecnología, sino un problema de riesgos y las diferentes maneras de comprenderlos y manejarlos. [13]

[13] Cano, J. (2004).Inseguridad informática: un concepto dual en seguridad informática. Obtenida el 12 de marzo de 2011, de http://www.virusprot.com/art47.html

Mientras más se conoce la inseguridad informática más se comprenden las acciones y resultados de la seguridad en las organizaciones. En este sentido, la detección de posibles problemas de seguridad generaría valor sin una adecuada respuesta. Una respuesta que reconozca la inseguridad informática como insumo y el ataque de seguridad como una variante a considerar en la protección de los activos. En consecuencia cuando somos capaces de reconocer y actuar en situaciones inesperadas, nuestra capacidad de análisis y control aumenta, pues nuevas perspectivas se abren a las relaciones que exhibe la inseguridad informática.

Finalmente las palabras "impenetrable", "invulnerable" o "seguro", nos recuerdan que existen procesos, muchas veces ocultos a nuestro pensamiento, que pondrán a prueba la realidad de los sistemas y sus propiedades. La inseguridad informática es pues una estrategia de reflexión y acción para repensar la seguridad informática como una disciplina que es al mismo tiempo sentimiento y realidad. [14]

6.1.1.6. Políticas de seguridad

Conjunto de normas, reglas procedimientos y prácticas que regulan la protección de la información contra la perdida de confidencialidad, integridad o disponibilidad, tanto de forma accidental como intencionada. [15]

Las políticas de seguridad informática surgen como una herramienta para concienciar a los colaboradores de la organización sobre la importancia y sensibilidad de la información.

Lo básico para exigir a los informáticos es tener redactada una política, que debe ser algo vivo, un documento escrito, consensuado por los jefes, con amplia participación del área de sistemas.

[14] Cano, J. (2004).Inseguridad informática: un concepto dual en seguridad informática. Obtenida el 12 de marzo de 2011, de http://www.virusprot.com/art47.html

[15] Chávez, A. (2009).Seguridad informática. Obtenida el 14 de septiembre de 2010, de http://www.biblioteca.clacso.edu.ar/recursos/seguridad-informatica.pdf.

Lo que suele pasar en la realidad es que no existe dicha política por escrito en las instituciones, tan solo existen políticas orales esto se debe a que la primera barrera que se enfrenta es convencer a los altos ejecutivos de la necesidad y beneficios de buenas prácticas de seguridad informática.

Proponer una política de seguridad requiere un alto compromiso con la organización, agudeza técnica en la identificación de vulnerabilidades y constancia para renovar y actualizar dicha política.

Actualmente las legislaciones nacionales de los Estados, obligan a las empresas, instituciones públicas a implantar una política de seguridad. Ej.: En España la Ley Orgánica de Protección de Datos o también llamada LOPD y su normativa de desarrollo. Generalmente se ocupa exclusivamente a asegurar los derechos de acceso a los datos y recursos con las herramientas de control y mecanismos de identificación. Estos mecanismos permiten saber que los operadores tienen sólo los permisos que se les dio. [16]

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

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

Los derechos de acceso de los operadores deben ser definidos por los responsables jerárquicos y no por los administradores informáticos, los cuales tienen que conseguir que los recursos y derechos de acceso sean coherentes con la política de seguridad definida.

[16] Wikipedia. (n.d).Seguridad informática. Obtenida el 14 de septiembre de 2010, de http://es.wikipedia.org/wiki/seguridad_ inform%C3%A1tica.

Además, como el administrador suele ser el único en conocer perfectamente el sistema, tiene que derivar a la directiva cualquier problema e información relevante sobre la seguridad, y eventualmente aconsejar estrategias a poner en marcha, así como ser el punto de entrada de la comunicación a los trabajadores sobre problemas y recomendaciones en término de seguridad informática.

La política de seguridad se expresa mediante principios y objetivos. Un principio es una norma o idea fundamental que rige la política de seguridad, y que se acepta en esencia. Un objetivo de seguridad es la declaración expresa de la intención de conseguir algo que contribuye a la seguridad de la información, bien porque se opone a una de las amenazas identificadas o bien porque satisface una exigencia de la política de seguridad de la información.

6.1.1.6.1. Importancia de las políticas de seguridad

Las políticas de seguridad en cómputo tienen como objeto establecer las medidas de índole técnica y de organización, necesarias para garantizar la seguridad de las tecnologías de la información (equipos de cómputo, sistemas de información, redes) y personas que interactúan haciendo uso de los servicios asociados a ellos y se aplican a todos los usuarios de cómputo de la institución.

Cada institución es responsable de dar a conocer y hacer cumplir estas políticas de seguridad internamente.

Una política de seguridad informática es una forma de comunicarse con los usuarios, ya que las mismas establecen un canal formal de actualización del personal, en relación con los recursos y servicios informáticos de la organización.[17]

[17] Chávez, A. (2009).Seguridad informática. Obtenida el 14 de septiembre de 2010, de http://www.biblioteca.clacso.edu.ar/recursos/seguridad-informatica.pdf.

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

6.1.2. Computación forense

6.1.2.1. Definición

El cómputo forense, también llamado informática forense, es la aplicación de técnicas científicas y analíticas especializadas a infraestructura tecnológica que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal.

Dichas técnicas incluyen reconstruir el bien informático, examinar datos residuales, autenticar datos y explicar las características técnicas del uso aplicado a los datos y bienes informáticos.

Como la definición anterior lo indica, esta disciplina hace uso no solo de tecnología de punta para poder mantener la integridad de los datos y del procesamiento de los mismos; sino que también requiere de una especialización y conocimientos avanzados en materia de informática y sistemas para poder detectar dentro de cualquier dispositivo electrónico lo que ha sucedido.[18]

[18] Wikipedia. (n.d).Computación forense. Obtenida el 05 de noviembre de 2010, de http://es.wikipedia.org/wiki/C%C3%B3mputo_forense.

6.1.2.2. Procedimientos del análisis forense

Análisis de computación forense

Las actividades a desarrollar por el profesional de la informática forense deben servir para la correcta planificación preventiva de seguridad de una red corporativa. En la medida que la Internet crece, lo hace de igual manera el número de acciones incursivas ilegales contra la seguridad de las redes corporativas.

Es importante y necesario planificar, analizar e implantar sistemas y políticas de seguridad, establecer medidas de control, planes de contingencia y realizar auditorías sobre los sistemas implantados y su correcto cumplimiento. Auditar las políticas de seguridad instituidas en la empresa, que tienen como objetivos analizar el nivel de cumplimiento de las políticas puestas en marcha y detectar aquellas lagunas para evolucionar en las mismas. Es así, como un procedimiento forense digital busca, precisamente, evitar esas modificaciones de los datos contenidos en el medio magnético al analizar, que se pueden presentar en cualquier instante, desde el mismo momento en el que haya ocurrido el presunto hecho punible por razones tan diversas al simple paso del tiempo, porque alguien haya decidido apagar la máquina, por que se haya ejecutado en ella una aplicación que sobre escribió en el almacenamiento de material informático y su correspondiente identificación para el peritaje por parte del personal policial; es así como debe ser efectuado conforme a las pautas elaboradas por los procedimientos Informáticos. Es de especial importancia la utilización de procedimientos rigurosos al momento del secuestro del material y de aquellos medios tendientes a garantizar la autenticidad e integridad de la evidencia digital estándar; aprobados para una mayor y eficaz solución. [19]

[19] Contreras, F. (2009).Herramientas de computación forense. Obtenida el 17 de marzo de 2011, de http://www.monografias.com/trabajos74/herramientas-computación-forense-control-digital.shtml.

El proceso de análisis forense a una computadora se describe a continuación:

Identificación

Es muy importante conocer los antecedentes, situación actual y el proceso que se quiere seguir para poder tomar la mejor decisión con respecto a las búsquedas y la estrategia de investigación. Incluye muchas veces la identificación del bien informático, su uso dentro de la red, el inicio de la cadena de custodia (proceso que verifica la integridad y manejo adecuado de la evidencia), la revisión del entorno legal que protege el bien y del apoyo para la toma de decisión con respecto al siguiente paso una vez revisados los resultados.

Preservación

Este paso incluye la revisión y generación de las imágenes forenses de la evidencia para poder realizar el análisis. Dicha duplicación se realiza utilizando tecnología de punta para poder mantener la integridad de la evidencia y la cadena de custodia que se requiere. Al realizar una imagen forense, nos referimos al proceso que se requiere para generar una copia “bit a bit” de todo el disco, el cual permitirá recuperar en el siguiente paso, toda la información contenida y borrada del disco duro. Para evitar la contaminación del disco duro, normalmente se ocupan bloqueadores de escritura de hardware, los cuales evitan el contacto de lectura con el disco, lo que provocaría una alteración no deseada en los medios.

Análisis

Proceso de aplicar técnicas científicas y analíticas a los medios duplicados por medio del proceso forense para poder encontrar pruebas de ciertas conductas. Se pueden realizar búsquedas de cadenas de caracteres, acciones específicas del o de los usuarios de la máquina como son el uso de dispositivos de USB, búsqueda de archivos específicos, recuperación e identificación de correos electrónicos, recuperación de los últimos sitios visitados y recuperación del caché del navegador de Internet.

Presentación

Es el recopilar toda la información que se obtuvo a partir del análisis para realizar el reporte y la presentación a los abogados, la generación (si es el caso) de una pericial y de su correcta interpretación sin hacer uso de tecnicismos. [20]

6.1.2.3. Herramientas de computación forense

La realidad competitiva de las empresas hace imprescindible para ellas acoplarse a las tecnologías de seguridad de la información disponibles, por lo que es prioritario que las empresas tomen medidas para proteger su información estratégica tanto de ataques internos como externos y a todos los niveles.

Es importante saber y conocer que es la informática forense dentro de la seguridad de una empresa o institución, mostrando para ello, algunas herramientas vitales en el área. Pero, la informática forense va mucho más allá de verificar e identificar la intrusión o ataque en los sistemas informáticos de una empresa, una labor importante es adiestrar y concienciar al personal involucrado dentro de la red organizativa indicando las medidas preventivas a seguir para evitar que la información de la empresa sea vulnerable.

Las actividades a desarrollar por el profesional de la informática forense deben servir para la correcta planificación preventiva de seguridad de una red corporativa.

[20] Wikipedia. (n.d).Computación forense. Obtenida el 05 de noviembre de 2010, de http://es.wikipedia.org/wiki/C%C3%B3mputo_forense.

En la medida que la Internet crece, lo hace de igual manera el número de acciones incursivas ilegales contra la seguridad de las redes corporativas. [21]

Una herramienta para software es una herramienta lógica o intangible, nos permite depurar, o diseñar nuevo software, se necesita cierto entrenamiento para poder usarla ya que generalmente se utiliza para tareas complicadas. No se daña con el uso, y se puede mejorar sin necesidad de adquirir otra.

Hablar de informática forense sin revisar algunas ideas sobre herramientas es hablar en un contexto teórico de procedimientos y formalidades legales. Las herramientas informáticas, son la base esencial de los análisis de las evidencias digitales en los medios informáticos. Sin embargo, es preciso comentar que éstas requieren de una formalidad adicional que permita validar tanto la confiabilidad de los resultados de la aplicación de las mismas, como la formación y conocimiento del investigador que las utiliza**.** [22]

En los últimos dos años se ha disparado el número de herramientas para computación forense, es posible encontrar desde las más sencillas y económicas, como programas de menos de US$300,00 cuyas prestaciones habitualmente son muy limitadas, hasta herramientas muy sofisticadas que incluyen tanto software como dispositivos de hardware.

Con esa amplia gama de alternativas, si se piensa adquirir una herramienta para computación forense, es necesario tener claro el objetivo que se persigue, pues existen varios tipos básicos de herramientas, no todos los productos sirven para todo, algunos están diseñados para tareas muy especificas y más aún, diseñados para trabajar sobre ambientes muy específicos, como determinado sistema operativo.

---

[21] Contreras, F. (2009).Herramientas de computación forense. Obtenida el 17 de marzo de 2011, de http://www.monografias.com/trabajos74/herramientas-computación-forense-control-digital.shtml.

[22] Cano, J. (2006).Introducción a la informática forense, una disciplina técnico-legal. Obtenida el 27 de febrero de 2011, de http://www.acis.org.co/fileadmin/Revista_96/dos.pdf.

Siendo la recolección de evidencia una de las tareas más críticas, donde asegurar la integridad de esta es fundamental, es necesario establecer ese nivel de integridad esperado, pues algunas herramientas no permiten asegurar que la evidencia recogida corresponda exactamente a la original. Igual de importante es que durante la recolección de la evidencia se mantenga inalterada la escena del "crimen". [23]

Dentro de las herramientas frecuentemente utilizadas en procedimientos forenses en informática se detallan algunas las cuales son aplicaciones que tratan de cubrir todo el proceso en la investigación forense en informática:

Encase - http://www.encase.com/products/ef_index.asp
Forensic Toolkit - http://www.accessdata.com/products/utk/
Winhex - http://www.x-ways.net/forensics/index-m.html

Si bien las herramientas detalladas anteriormente son licenciadas y sus precios oscilan entre los 600 y los 5000 dólares americanos, existen otras que no cuentan con tanto reconocimiento internacional en procesos legales, que generalmente son aplicaciones en software de código abierto:

Sleuth Kit -http://www.sleuthkit.org/Coroner
Toolkit http://www.porcupine.org/forensics/tct.html

Estás últimas a pesar de que son utilizadas con frecuencia como estrategia de validación en el uso de otras herramientas, vienen haciendo una importante carrera en la práctica de la informática forense, con lo cual no se descarta en un futuro próximo que éstas estén compitiendo mano a mano con las herramientas de código cerrado mencionadas anteriormente. [24]

[23] Asobancaria.(2004).La informática forense y la banca. Obtenida el 17 de marzo de 2011, de http://www.asobancaria.com/upload/docs/docPag1993_1.pdf.

[24] Cano, J. (2006).Introducción a la informática forense, una disciplina técnico-legal. Obtenida el 27 de febrero de 2011, de http://www.acis.org.co/fileadmin/Revista_96/dos.pdf.

6.1.2.3.1. Herramienta Nessus

6.1.2.3.1.1. Historia

El proyecto de "Nessus" fue iniciado por Renaud Deraison en 1998 para proporcionar al internet una comunidad remota de escáner de seguridad gratuito. El 5 de octubre de 2005, Tenable Network Security (Seguridad de red sostenible), la compañía que fue cofundada por Renaud Deraison, cambió Nessus 3 a un software de de código cerrado es decir con licencia. El instalador de Nessus 3 sigue siendo de forma gratuita, aunque las comisiones de la compañía tienen un precio de $ 100 al mes por cada escáner para obtener la capacidad de realizar auditorías de configuración de PCI, la CEI, FDCC y la configuración de otras normas, el apoyo técnico, auditorías de la vulnerabilidad, la red de controles y auditorías de última revisión, la capacidad de auditoría de configuraciones anti-virus y la capacidad de Nessus para realizar búsquedas de datos sensibles. Nessus 3 está disponible para diversos sistemas Unix y Windows, ofrece la auditoría de parches de Unix.

6.1.2.3.1.2. ¿Qué es Nessus?

Nessus no es una herramienta que se utiliza durante el procedimiento del análisis forense, es una herramienta de evaluación de seguridad. Nessus es considerado el mejor escáner de vulnerabilidades del mundo, podría decirse que los demás se basan en este. Nessus es el líder mundial en escáneres de activos se estima que es utilizado por más de 75,000 organizaciones en el mundo, con el descubrimiento de alta velocidad, la auditoría de configuración, el perfil activo, el descubrimiento de los datos sensibles y análisis de la vulnerabilidad de su seguridad. [25]

[25] Tenable Network Security. (2002).Nessus. Obtenida el 05 de noviembre de 2010 de http://www.nessus.org/products/nessus.

Nessus se puede distribuir a lo largo de toda una empresa, dentro de DMZ y a través de redes separadas físicamente; en entornos empresariales Nessus se usa mucho para analizar sus propios equipos en lo que se llama una "Auditoria de Seguridad Interna", es gratuito para uso personal en un entorno no empresarial.

6.1.2.3.1.3. Funcionamiento

En funcionamiento normal, Nessus comienza haciendo un escaneo de puertos con uno de sus cuatro portscanners (escáneres de puerto) internos y opcionalmente puede utilizar Nmap para determinar qué puertos están abiertos. Las pruebas de vulnerabilidad, disponibles como suscripciones, están escritos en NASL (Nessus Attack Scripting Language), un lenguaje de scripting optimizado para la interacción de red personalizada.

La compañía Tenable Network Security produce varias docenas de nuevas comprobaciones de vulnerabilidad (llamados plugins) cada semana, generalmente sobre una base diaria. Estos controles están disponibles de forma gratuita al público en general, los clientes comerciales no están autorizados a utilizar esta casa de alimentación. Las actualizaciones a la base de datos (que no son gratis) también dan acceso y apoyo a secuencias de comandos adicionales (y el cumplimiento de las pruebas de auditoría). Opcionalmente, los resultados de la exploración pueden ser reportados en varios formatos, como texto plano, XML, HTML y LaTeX. Los resultados también se pueden guardar en una base de conocimientos para la depuración.[26]

[26] Tenable Network Security. (2002).Nessus. Obtenida el 05 de noviembre de 2010 de http://www.nessus.org/products/nessus.

En Unix, la exploración se puede automatizar mediante el uso de un cliente de línea de comandos. Nessus proporciona funcionalidad adicional más allá de las pruebas de vulnerabilidades de la red conocida. Por ejemplo, puede utilizar Windows para examinar las credenciales de los niveles de revisión en equipos que ejecutan el sistema operativo Windows, también puede auditar los sistemas para asegurarse de que se han configurado por una política específica, como la NSA para endurecer los servidores Windows.

Nessus descubre los dispositivos de red e identifica los sistemas operativos, aplicaciones, bases de datos y servicios que se ejecutan sobre dichos activos. Las máquinas que no cumplen, como los sistemas que ejecutan P2P, spyware o malware (gusanos, troyanos, entre otros) son detectados e identificados. Nessus es capaz de escanear todos los puertos de cada dispositivo y sugiere estrategias de rehabilitación según sea necesario. Nessus incluye la capacidad de realizar auditorías de aplicaciones web en profundidad, identificar las vulnerabilidades en aplicaciones personalizadas. Las aplicaciones personalizadas pueden tener su web, sistemas operativos, aplicaciones y base de datos SQL auditados y endurecidos, de acuerdo a una variedad de recomendaciones de buenas prácticas de la CEI y DISA.

Nessus proporciona la capacidad de datos para identificar con precisión las configuraciones de sistema de inventario. Cuando los datos se gestionan por el centro de seguridad de la compañía, proporciona informes de los sistemas de auditoría para el cumplimiento normativo.

Las auditorías de las redes de menos de 100 hosts se pueden completar en pocos minutos. Esto se puede lograr con un ordenador portátil o un servidor de potencia media. [27]

[27] Tenable Network Security. (2002).Nessus. Obtenida el 05 de noviembre de 2010 de http://www.nessus.org/products/nessus.

Nessus continuamente puede escanear los dispositivos de red para ahorrar drásticamente el tiempo de identificación de las vulnerabilidades que puedan surgir. Nessus puede analizar los sistemas sin necesidad de credenciales administrativas, y también pueden probar con técnicas de explotación según sea necesario. Si las credenciales se proporcionan durante la auditoría, Nessus puede determinar una lista exacta de los desaparecidos parches y errores de configuración.

Nessus tiene una variedad de controles que tratan de identificar las infecciones de virus específicos y puertas traseras a través de la interacción con un servicio de red. El mejor ejemplo de esto es el plugin #36217 que detecta el servicio de Conficker P2P. Nessus también busca en los servidores web para ver si está recibiendo JavaScript con conocidos vínculos hostiles que pueden indicar que usted puede tener un servidor web comprometido.

Nessus también tiene otras formas de servicio de detección genérica de virus. El primero es el plugin #33950 que evalúa los datos transmitidos de un servicio para ver si se trata de un ejecutable de Microsoft. Algunos otros ejemplos de plugins que detectan indicios de un virus, una infección o compromiso:

- plugin #33950 encuentra un archivo ejecutable que se sirve en la red y que probablemente tenga algún tipo de compromiso.
- Plugin #35322 controles para los ejecutables que se sirve por los servidores web.
- plugins #33951 mira a las banderas reales en los servicios que se escanea y busca indicios de que estas banderas son de conocidos demonios comprometida. [28]

[28] Tenable Network Security. (2002).Nessus. Obtenida el 05 de noviembre de 2010 de http://www.nessus.org/products/nessus.

Nessus tiene varios plugins que identifican soluciones para antivirus y comprueba si su base de firmas está fuera de fecha. La lista de los antivirus incluye:

- BitDefender
- Eset Nod32
- Kaspersky
- McAfee
- Panda
- Sophos
- Symantec
- Trend Micro
- Windows Live OneCare

Nessus plugins #45051 enumera el software antivirus en un servidor Windows a través de un instrumental de administración de Windows. Nessus también comprueba las vulnerabilidades de muchos agentes antivirus. Estos controles están disponibles para los usuarios con suscripción de HomeFeed y ProfessionalFeed.

6.1.2.3.1.4. Licencia de Nessus

Las organizaciones comerciales que utilizan el escáner de vulnerabilidades Nessus deben comprar una suscripción de ProfessionalFeed para escanear su red, obtener el apoyo, las actualizaciones de su base de datos de los controles de la vulnerabilidad y la auditoría de cumplimiento. Cada ProfessionalFeed cuesta $ 1,200 por año por cada escáner Nessus y se pueden adquirir directamente desde el comercio electrónico del sitio . En julio de 2008, la compañía envió una revisión de la licencia de alimentación que permitirá a los usuarios acceso total a su casa de plugins. [29]

[29] Obtenido de Wikipedia. (n.d). Nessus. Obtenida el 05 de noviembre de 2010, de http://es.wikipedia.org/wiki/Nessus y Tenable Network Security. (2002).Nessus. Obtenida el 05 de noviembre de 2010 de http://www.nessus.org/products/nessus.

6.1.3. Norma ISO 27001

6.1.3.1. Origen

En 1995 el British Standard Institute publica la norma BS 7799, un código de buenas prácticas para la gestión de la seguridad de la información.

En 1998, también el BSI publica la norma BS 7799-2, especificaciones para los sistemas de gestión de la seguridad de la información; se revisa en 2002.

Tras una revisión de ambas partes de BS 7799 (1999), la primera es adoptada como norma ISO en 2000 y denominada ISO/IEC 17799:

1. Conjunto completo de controles que conforman las buenas prácticas de seguridad de la información.

2. Aplicable por toda organización, con independencia de su tamaño.

3. Flexible e independiente de cualquier solución de seguridad concreta:

En 2002 la norma ISO se adopta como UNE sin apenas modificación (UNE 17799). [30]

El 15 de Octubre de 2005 se publica la norma ISO 27001, esta es la principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información (SGSI).

[30] Villalón, A. (2004).Códigos de buenas prácticas de seguridad. UNE-ISO/IEC 17799. Obtenida el 17 de septiembre de 2010, de http://wwww.shutdown.es/ISO177799.pdf.

Tiene su origen en la BS 7799-2:2002 y es la norma con arreglo a la cual se certifican por auditores externos los SGSI de las organizaciones. Sustituye a la BS 7799-2, habiéndose establecido unas condiciones de transición para aquellas empresas certificadas en esta norma. [31]

En su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005 (nueva numeración de ISO 17799:2005 desde el 1 de Julio de 2007), para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI; a pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados. Desde el 28 de Noviembre de 2007, esta norma está publicada en España como UNE- ISO/IEC 27001:2007.

6.1.3.2. Definición

La norma ISO 27001 es una norma internacional que ofrece recomendaciones para realizar la gestión de la seguridad de la información dirigidas a los responsables de iniciar, implantar y mantener la seguridad de una organización. [32]

Este es un estándar preparado para proveer un modelo de establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y mejora de un Sistema de Gestión de Seguridad de la Información documentado; en el contexto de los riesgos específicos de las actividades de la organización. [33]

---

[31] Chacón, D. (2009).Norma ISO 27001 Informe. Obtenida el 05 de octubre de 2010, de http://djeffersec.site11.com/web_documents/ISO%2027001.pdf.

[32] ISO27000.es. (n.d).El portal de ISO 27001 en Español. Obtenida el 05 de noviembre de 2010, de http://www.ISO27000.ES.

[33] Scribd. (2010).ISO 27000.Obtenida el 05 de octubre de 2010, de http://es.scribd.com/doc/40168939/Doc-Iso27000-All.

El enfoque a Procesos para la gestión de seguridad de información que se presenta en éste Estándar Internacional enfatiza la importancia de:

1. Entender los requerimientos de seguridad de una organización y la necesidad de establecer políticas y objetivos para la seguridad de la información.
2. Implementar y operar controles para manejar la los riesgos de seguridad de la información.
3. Monitorear y revisar el rendimiento del Sistema de Gestión de seguridad de la información.
4. Mejoramiento continuo, éste estándar adopta un modelo “Planear-Hacer-Revisar-Actuar” que se aplica para estructurar todos los procesos del SGSI. [34]

Esta norma define la información como un activo que posee valor para la organización y requiere por tanto de una protección adecuada. El objetivo de la seguridad de la información es proteger adecuadamente este activo para asegurar la continuidad del negocio minimizar los daños a la organización y maximizar el retorno de las inversiones y las oportunidades de negocio.

La seguridad de la información se define como la preservación de:

1. Confidencialidad: Aseguramiento de que la información es accesible sólo para aquellos autorizados a tener acceso.
2. Integridad: Garantía de la exactitud y completitud de las información y de los métodos de su procesamiento.
3. Disponibilidad: Aseguramiento de que los usuarios autorizados tienen acceso cuando requieran información y sus activos asociados.

[34] Chacón, D. (2009).Norma ISO 27001 Informe. Obtenida el 05 de octubre de 2010, de http://djeffersec.site11.com/web_documents/ISO%2027001.pdf.

6.1.3.3. Estructura de la norma

La norma UNE-ISO/IEC 27001 establece once dominios de control que cubren por completo la gestión de la seguridad de la información, para cada uno de ellos se define el objetivo y lo describe brevemente. [35]

Un "control" es lo que permite garantizar que cada aspecto, que se valoró con un cierto riesgo, queda cubierto y auditable.

Los controles que el anexo A de esta norma propone quedan agrupados y numerados de la siguiente forma:

A.5 Políticas de seguridad

A.6 Aspectos organizativos de la seguridad de la información

A.7 Administración de recursos

A.8 Seguridad de los recursos humanos

A.9 Seguridad física y del entorno

A.10 Administración de las operaciones y las comunicaciones

A.11 Control de accesos

A.12 Adquisición de sistemas de información, desarrollo y mantenimiento

A.13 Administración de los incidentes de seguridad

A.14 Administración de la continuidad del negocio

A.15 Cumplimiento (legales, de estándares, técnicas y auditorias)

[35] ISO27000.es. (n.d).El portal de ISO 27001 en Español. Obtenida el 05 de noviembre de 2010, de http://www.ISO27000.ES.

A.5 Política de seguridad

Documento de política de seguridad y su gestión, este control tiene como objetivo dirigir y dar soporte a la gestión de la seguridad de la información.

A.6 Aspectos organizativos de la seguridad de la información

Este control establece que debe diseñarse una estructura organizativa dentro de la compañía que defina responsabilidades que en materia de seguridad tiene cada usuario o área de trabajo relacionada con los sistemas de información de cualquier forma, dicha estructura debe poseer un enfoque multidisciplinar: Los problemas de seguridad no son exclusivamente técnicos.

A.7 Administración de recursos

Responsabilidad sobre los activos; asegurar un nivel de protección adecuado a los activos de información.

Debe definirse una clasificación de los activos relacionados con los sistemas de información, manteniendo un inventario actualizado que registre esos datos y proporcione a cada activo el nivel de protección adecuado a su criticidad en la organización.

A.8 Seguridad de los recursos humanos

Para garantizar que los empleados, contratistas y terceros usuarios entiendan sus responsabilidades y funciones que se consideran para ellos, para reducir el riesgo de robo, fraude o uso indebido de las instalaciones, se define roles, responsabilidades, proyección, términos y condiciones de trabajo.

Asegurar que los usuarios son conscientes de las amenazas y riesgos en el ámbito de la seguridad de la información y que están preparados para sostener la política de seguridad de la organización en el curso normal de su trabajo.[36]

[36]ISO27000.es. (n.d).El portal de ISO 27001 en Español. Obtenida el 05 de noviembre de 2010, de http://www.ISO27000.ES.

A.9 Seguridad física y del entorno

Áreas seguras: proceso para prevenir el acceso físico no autorizado, daño o interferencia a las premisas e información de la organización.

Seguridad del equipamiento: para evitar la pérdida, daño, robo o compromiso de los activos y la interrupción de las actividades de la organización.

A.10 Administración de las operaciones y las comunicaciones

Responsabilidades y procedimientos de operación; gestión de la provisión de servicios por terceros; planificación y aceptación del sistema; protección contra código malicioso y descargable; Copias de seguridad; gestión de seguridad de las redes y manipulación de los soportes.

A.11 Control de accesos

Requisitos de negocio para el control de acceso; gestión de acceso de usuario; control de acceso a la red; control de acceso al sistema operativo y control de acceso a las aplicaciones y a la información.

A.12 Adquisición de sistemas de información, desarrollo y mantenimiento

Requisitos de seguridad de los sistemas de información; tratamiento correcto de las aplicaciones; controles criptográficos y seguridad de los archivos de sistema.

A.13 Administración de los incidentes de seguridad

Notificación de eventos y puntos débiles de la seguridad de la información; gestión de incidentes de seguridad de la información y mejoras.[37]

[37] ISO27000.es. (n.d).El portal de ISO 27001 en Español. Obtenida el 05 de noviembre de 2010, de http://www.ISO27000.ES.

A.14 Administración de la continuidad del negocio

Aspectos de la seguridad de la información en la gestión de la continuidad del negocio.

La organización debe de reaccionar a la interrupción de actividades del negocio y proteger sus procesos críticos frente a grandes fallos o desastres. Todas las situaciones que puedan provocar la interrupción de las actividades del negocio deben ser prevenidas y contra restadas mediante los planes de contingencia.

A.15 Cumplimiento (legales, de estándares, técnicas y auditorias)

Cumplimiento de los requisitos legales; cumplimiento de las políticas, normas de seguridad, cumplimiento técnico; consideraciones sobre las auditorias de los sistemas de información.[38]

[38]. ISO27000.es. (n.d).El portal de ISO 27001 en Español. Obtenida el 05 de noviembre de 2010, de http://www.ISO27000.ES.

6.1.3.4. Dominios de control (A.5, A.7, A.9, A.10, A.11, A.12)

A.5 Política de seguridad

Su objetivo es proporcionar orientación y apoyo a la gestión de seguridad de la información de acuerdo con las empresas, requisitos, leyes y reglamentos pertinentes.

La política de seguridad, para ser rigurosa, en realidad debería dividirse en dos documentos:

- Política de seguridad (Nivel político o estratégico de la organización): Es la mayor línea rectora, la alta dirección define las grandes líneas a seguir y el nivel de compromiso de la dirección con ellas.
- Plan de seguridad (Nivel de planteamiento): Define el "cómo". Es decir, baja a un nivel más de detalle, para dar inicio al conjunto de acciones o líneas rectoras que se deberán cumplir.

Algo sobre lo que generalmente no se suele reflexionar o marcar es que:

- Una "política de seguridad "bien planteada, diseñada y desarrollada cubre la gran mayoría de los aspectos que hacen falta para un verdadero SGSI.
- La alta dirección debe definir una política que refleje las líneas directrices de la organización en materia de seguridad, aprobarla y publicitarla de la forma adecuada a todo el personal implicado en la seguridad de la información.
- La política se constituye en la base de todo el sistema de seguridad de la información, la alta dirección debe apoyar visiblemente la seguridad de la información de la compañía.[39]

[39] Obtenido de Corletti, A. (2006).ISO-27001: Los controles (Parte I).Obtenida el 13 de octubre de 2010, de http://www.delitosinformaticos.com/11/2006/seguridad-informatica/iso-27001-los-controles-parte-i.

A.7 Administración de recursos

Responsabilidad en los recursos: Inventario de los recursos y empleo aceptable de los mismos.

Este control es inminente, procedimental y no aporta nada al aspecto ya conocido en seguridad de la información, en cuanto a que todo recurso debe estar perfectamente inventariado con el máximo detalle posible; se debe documentar el uso adecuado de los recursos y toda la información deberá ser tratada de acuerdo a su nivel.

No se puede pensar en seguridad, si no se conoce con exactitud lo que posee la institución y cada elemento que no se ha inventariado, es un hueco concreto en la seguridad de todo el sistema y de hecho suelen ser las mayores y más frecuentes puertas de entrada, pues están al margen de la infraestructura de seguridad. [40]

A.9 Seguridad física y del entorno

Este control se encuentra subdividido en:

- Áreas de seguridad: Seguridad física y perimetral; control físico de entradas; seguridad de los locales, edificios y recursos; protección contra amenazas externas y del entorno; accesos públicos; áreas de entrega y carga.
- Seguridad de elementos: Ubicación y protección de equipos, elementos de soporte a los equipos, seguridad en el cableado, mantenimiento de los equipos, seguridad en el equipamiento fuera de la organización, seguridad en la redistribución o reutilización de equipamiento.

[40] Obtenido de Corletti, A. (2006).ISO-27001: Los controles (Parte I).Obtenida el 13 de octubre de 2010, de http://www.delitosinformaticos.com/11/2006/seguridad-informatica/iso-27001-los-controles-parte-i.

- Empleo correcto del material informático y de comunicaciones a nivel físico se deben desarrollar en este control, cuales son las medidas de seguridad física que se deben tener en cuenta sobre los mismos (ubicación, acceso al mismo, tensión eléctrica, conexione físicas, hardware permitido o prohibido, manipulación de elementos). No se incluye aquí lo referente a la seguridad lógica.

- Seguridad física en el almacenamiento y transporte de material informático y de comunicaciones: Zonas y medidas de almacenamiento; metodología a seguir para el ingreso y egreso de este material; consideraciones particulares para transporte del mismo (dentro y fuera de la organización); personal autorizado a recibir, entregar o sacar material; medidas de control. No se incluye aquí lo referido a resguardo y recuperación de información que es motivo de otro tipo de procedimientos y normativas.

A.10 Administración de las operaciones y las comunicaciones

Este control se divide en:

- Procedimientos, operaciones y responsabilidades: Garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información.

- La planificación del sistema y la aceptación: Minimizar el riesgo de fallos en los sistemas.[41]

- Protección contra código malicioso y móvil: Proteger la integridad del software y la información.

- Respaldos: Para mantener la integridad y la disponibilidad de la información y del acceso a ella.

[41] Obtenido de Corletti, A. (2006).ISO-27001: Los controles (Parte I).Obtenida el 13 de octubre de 2010, de http://www.delitosinformaticos.com/11/2006/seguridad-informatica/iso-27001-los-controles-parte-i y Corletti, A. (2007).ISO-27001: Los controles (Parte II).Obtenida el 13 de octubre de 2010, de http://www.delitosinformaticos.com/01/2007/seguridad-informatica/iso-27001-los-controles-parte-ii.

- Monitoreo: Para detectar el acceso a información no autorizada o a procesos no autorizados.
- Asegurar la salvaguarda de la información en las redes y la protección de su infraestructura de apoyo.
- Evitar daños a los activos e interrupciones de actividades de la organización.
- Prevenir la perdida, modificación o mal uso de la información intercambiada entre organizaciones.

También se hace hincapié en documentar todos los procedimientos, manteniendo los mismos y disponibles a todos los usuarios que los necesiten, segregando adecuadamente los servicios y las responsabilidades para evitar el uso inadecuado de los mismos.

A.11 Control de accesos

Este control tiene como objetivo controlar los accesos a la información. Se deben establecer los controles de acceso adecuados para proteger los sistemas de información críticos para el negocio, a diferentes niveles: Sistema operativo, aplicaciones y redes.

No se debe confundir la actividad de control de accesos con autenticación, esta última tiene por misión identificar que verdaderamente "sea, quien dice ser". El control de acceso es posterior a la autenticación y debe regular que el usuario autenticado, acceda únicamente a los recursos sobre los cuales tenga derecho y a ningún otro, es decir que tiene dos tareas derivadas:[42]

- Encauzar (o enjaular) al usuario debidamente.
- Verificar el desvío de cualquier acceso fuera de lo correcto.

[42] Corletti, A. (2007).ISO-27001: Los controles (Parte II).Obtenida el 13 de octubre de 2010, de http://www.delitosinformaticos.com/01/2007/seguridad-informatica/iso-27001-los-controles-parte-ii.

El control de acceso es una de las actividades más importantes de la arquitectura de seguridad de un sistema. Al igual que sucede en el mundo de la seguridad física, para cumplir con este propósito, se precisa de ciertas especificaciones que se agrupa de la siguiente forma:

- Requerimientos de negocio para el control de accesos: Debe existir una Política de Control de accesos documentada, periódicamente revisada y basada en los niveles de seguridad que determine el nivel de riesgo de cada activo.

- Gestión de accesos de usuarios: Tiene como objetivo asegurar el correcto acceso y prevenir el no autorizado y, a través de cuatro controles, exige llevar un procedimiento de registro y revocación de usuarios, una adecuada administración de los privilegios y de las contraseñas de cada uno de ellos, realizando periódicas revisiones a intervalos regulares, empleando para todo ello procedimientos formalizados dentro de la organización.

- Responsabilidades de usuarios: Todo usuario dentro de la organización debe tener documentadas sus obligaciones dentro de la seguridad de la información de la empresa. Independientemente de su jerarquía, siempre tendrá alguna responsabilidad a partir del momento que tenga acceso a la información. [43]

[43] Corletti, A. (2007).ISO-27001: Los controles (Parte II).Obtenida el 13 de octubre de 2010, de http://www.delitosinformaticos.com/01/2007/seguridad-informatica/iso-27001-los-controles-parte-ii.

- Control de acceso a redes: Todos los servicios de red deben ser susceptibles de medidas de control de acceso; para ello a través de siete controles, en este grupo se busca prevenir cualquier acceso no autorizado a los mismos.

  Como primera medida establece que debe existir una política de uso de los servicios de red para que los usuarios, solo puedan acceder a los servicios específicamente autorizados. Luego se centra en el control de los accesos remotos a la organización, sobre los cuales deben existir medidas apropiadas de autenticación.

  Un punto sobre el que merece la pena detenerse es sobre la identificación de equipamiento y de puertos de acceso. Este aspecto es una de las principales medidas de control de seguridad.

- Control de acceso a sistemas operativos: Tiene que ver con la seguridad en la validación de usuarios al S.O, empleo de identificadores únicos de usuarios, correcta administración de contraseñas, control y limitación de tiempo en las sesiones y por ultimo verificación de empleo de utilidades de los S.O que permitan realizar acciones “interesantes”.

- Control de acceso a información y aplicaciones: Este sub control está dirigido a prevenir el acceso no autorizado a la información mantenida en las aplicaciones. Propone redactar, dentro de la política de seguridad, las definiciones adecuadas para el control de acceso a las aplicaciones y a su vez el aislamiento de los sistemas sensibles del resto de la infraestructura. [44]

[44] Corletti, A. (2007).ISO-27001: Los controles (Parte II).Obtenida el 13 de octubre de 2010, de http://www.delitosinformaticos.com/01/2007/seguridad-informatica/iso-27001-los-controles-parte-ii.

A.12 Adquisición de sistemas de información desarrollo y mantenimiento.

Debe contemplarse la seguridad de la información en todas las etapas del ciclo de vida del software en una organización: especificación de requisitos, desarrollo, explotación, mantenimiento.

- Procesamiento correcto en aplicaciones: El objetivo de este sub control es el correcto tratamiento de la información en las aplicaciones de la empresa ,las medidas a adoptar son: validación en la entrada de datos, la implementación de controles internos en el procesamiento de la información para verificar o detectar cualquier corrupción de la información a través de los procesos, tanto por error como intencionalmente, la validación en la salida de datos, para asegurar que los datos procesados, y su posterior tratamiento o almacenamiento, sea apropiado a los requerimientos de esa aplicación.

- Controles criptográficos: El objetivo de la criptografía de proteger la integridad, confidencialidad y autenticidad de la información. El tema de claves criptográficas, como se ha podido apreciar hasta ahora, es un denominador común de toda actividad de seguridad.

- Seguridad en los sistemas de archivos: La Seguridad en los sistemas de archivos, independientemente que existan sistemas operativos más robustos que otros en sus técnicas de archivos y directorios, es una de las actividades sobre las que se debe hacer un esfuerzo técnico adicional, pues en general existen muchas herramientas para robustecerlos, pero no suelen usarse.

- Administración técnica de vulnerabilidades: Toda vulnerabilidad que sucede en un sistema de información, tarde o temprano se debe describir , pues cuanto antes se tenga conocimiento de una debilidad y las medidas adecuadas para solucionarlas, mejor será para la organización.

6.1.3.5. Ventajas de la norma

La adopción de la norma ISO 27001 proporciona diferentes ventajas para cualquier organización:

1. Aumento de la seguridad efectiva de los sistemas de información.

2. Correcta planificación y gestión de la seguridad.

3. Garantías de continuidad del negocio.

4. Mejora continua a través del proceso de auditoría interna.

5. Incremento de los niveles de confianza de los clientes.

6. Aumento del valor comercial y mejora de la imagen de la Organización.[45]

[45] ISO27000.es. (n.d).El portal de ISO 27001 en Español. Obtenida el 05 de noviembre de 2010, de http://www.ISO27000.ES

6.1.4. Centro de cómputo

6.1.4.1. Definición

Es la unidad de servicio encargado del diseño e implementación de sistemas y de la administración de los recursos computacionales de la empresa. Su trabajo se enfoca hacia el desarrollo de herramientas que faciliten la labor del resto de dependencias de la empresa.

Las funciones básicas de un Centro de Cómputo son:

1. Realización de estudios de factibilidad.
2. Desarrollo de sistemas incluyendo: Análisis, diseño, implementación, control y documentación.
3. Brindar la capacitación necesaria a los usuarios para el correcto uso de las aplicaciones.
4. Dar mantenimiento a los sistemas y determinar mejoras.
5. Velar por el buen funcionamiento del equipo de cómputo.
6. Realizar las evaluaciones de las necesidades técnicas en software y hardware.
7. Asesorar a los otros departamentos en lo concerniente a procesamiento de datos. [46]

[46] Scribd. (2010).Administración de centros de cómputo. Obtenida el 05 de noviembre de 2010, de http:// es.scribd.com/doc/3081866/Administracion-de-Centros-de-Computo

6.1.4.2. Clasificación de un centro de cómputo

Se clasifica en tres: grandes, medianos y pequeño. Los parámetros para hacer esta clasificación son:

- Capacidad del hardware instalado
- Disponibilidad de las herramientas del software
- Clasificación del personal

También se pueden clasificar por su forma de proceso en:

- Centralizado
- Descentralizado

Los centralizados son aquellos que poseen un núcleo que comanda todos los demás, sin la activación de este, los demás nodos no pueden efectuar ningún proceso.

Los descentralizados son aquellos que no dependen de un solo núcleo, ya que se encuentra dividido en varios subsistemas.[47]

[47] Scribd. (2010).Administración de centros de cómputo. Obtenida el 05 de noviembre de 2010, de http:// es.scribd.com/doc/3081866/Administracion-de-Centros-de-Computo

6.2. Hipótesis

La toma de decisiones efectiva sobre la seguridad informática del centro de cómputo del Hospital Militar “Alejandro Dávila Bolaños” depende del proceso de planificación y gestión administrativa.

6.3. Diseño metodológico

1) Tipo de investigación

El tipo de investigación es descriptiva, está basada en la información recopilada antes y durante la investigación.

2) Técnica de análisis

La técnica que se utilizó para analizar los resultados obtenidos en la recolección de datos es el análisis cualitativo.

3) Técnicas de recolección de datos

En cuanto a las técnicas de recolección de información se utilizaron las siguientes:

- **a.** Se visitó el Hospital Militar con el objetivo de verificar el funcionamiento del centro de cómputo.
- **b.** Entrevista, cuestionario y petición de documentación concreta.
- **c.** Se consultaron diferentes sitios web y bibliografía para elaborar el marco teórico.

6.4. Desarrollo del subtema

6.4.1. Información general del Hospital Militar “ADB”

6.4.1.1. Antecedentes del Hospital Militar “ADB”

El hospital militar surge en el año 1956, creado por militares norteamericanas a través de una empresa mexicana. Formó parte de una serie de hospitales militares que se construyeron en ese tiempo a nivel centroamericano: El Salvador, Guatemala, Panamá, Nicaragua, de estos cuatro países el único que sigue funcionando como hospital militar en Nicaragua es el hospital militar "Alejandro Dávila Bolaños”.

En 1979, durante la insurrección popular, el hospital es abandonado por la Guardia Nacional que lo entrega a la Cruz Roja. El 19 de Agosto de 1979, la Cruz Roja lo entrega a las autoridades del nuevo Ejército de Nicaragua (denominado en ese momento Ejército Popular Sandinista), denominándose desde ese momento hospital militar "Alejandro Dávila Bolaños”, en honor a un médico e investigador indigenista asesinado en Estelí por la Guardia Nacional mientras realizaba una cirugía de emergencia.

Durante la década de los ochenta, el hospital se especializaba en la atención de heridas y traumatismos de los miembros del Ejército que se producían en acciones de combate.

Durante la década de los noventa, después de haberse logrado la paz, el hospital cambió su perfil transformándose en un Hospital General que atiende todo tipo de enfermedades y recibe pacientes militares y civiles que se encuentran adscritos al sistema de salud provisional del Instituto Nicaragüense de Seguridad Social.

El Hospital Militar ha completado un proceso de transformación que lo llevo a ser actualmente un hospital de perfil general dedicado a proporcionar servicios de muy alta calidad de segundo nivel a la población militar de todo el país y a proporcionar servicios médicos ambulatorios y de internación de alta calidad a la población civil de Managua.

6.4.1.2. Antecedentes del departamento de informática

El departamento de informática del hospital surge para los años 89 y 90, contaba con 4 o 5 computadoras en el área administrativa, eran máquinas que ya estaban obsoletas, esto era la continuidad de las máquinas de escribir en las oficinas. Para los años 98 y 99 se tenían de 13 a 21 computadoras en el área antes mencionada, poco después el desarrollo tecnológico presionó y se llegó a la conclusión que se tenía que crear una estructura de red y crear una unidad informática.

Para el año 2000 sólo una persona laboraba en el departamento de informática, no diseñaba programas, sólo manejaba algunos sistemas contables para el área administrativa tales como: finanzas, contabilidad y créditos. Estas eran áreas pequeñas todas se encontraban en una oficina, contaban con dos sistemas: El CONTEMPANE para contabilidad y el MEGAPACK para suministros médicos e inventarios.

Con la llegada del ingeniero Oscar Aguilar se formó el departamento con tres áreas específicas:

Mantenimiento y reparación con dos personas, sistemas con un analista y dos programadores y el área de redes con una persona.

El departamento de informática seguía creciendo no solamente en infraestructura sino en servicios con el objetivo de dar una mejor atención a los pacientes. Ese mismo año se crea un diseño de red que involucro a todas las áreas de servicios de informática del hospital, desarrollaron su propio software que les permitió brindar un servicio preciso a los pacientes desde que llegaban hasta que se retiraban del hospital.

Desde que surgió el departamento de informática se venía trabajando con la subdirección administrativa pero la creciente demanda que venía experimentando el hospital en cuanto al servicio informatizado no eran solucionados por que la subdirección administrativa no se reunía con el departamento de informática y no les orientaba sus funciones, tareas a realizar, por tal razón la junta directiva del hospital vio la necesidad de que el departamento de informática pasaría bajo el mando de la subdirección de planificación.

Este cambio sirvió para que se crearan dos sistemas más que son: El PAME programa de asegurados y cobertura se pudo realizar esta estrategia de hacer su propio software gracias a la ayuda de la subdirección de planificación, ya que ellos manejan el manual operativo de cada una de las áreas de servicio, y agilizo la realización de un diseño de red, un análisis en cada área para obtener los requerimientos de ellos.

El centro de computo se crea en el año 2004 era una de las tareas principales de la subdirección de planificación, se crea con el objetivo de lograr que la información esté disponible y centralizada. El centro de cómputo es un lugar que permite el acceso a los directivos del hospital a cada uno de los servidores instalados.

6.4.2. Objetivo del centro de cómputo del Hospital Militar “ADB”

Da asistencia técnica en cuanto a soporte de software y desarrollo sistemas para información médica y administrativa.

Las áreas que dependen del centro de cómputo son: caja, farmacia, administración, informática.

6.4.3. Metodología para la elaboración del plan de seguridad informática

6.4.3.1. Identificación de los activos informáticos de la institución

Cantidad	Activos	Descripción
192	Computadoras	Marca Dell y Compaq ; con sistema operativo Windows 98, Windows 2000 y Windows xp
56	Impresoras	Matriciales y de inyección
1	Conexión de red	Corporativo de IBW
1	Servidor de datos	Sistema operativo Windows NT
1	Servidor de SQL	Sistema operativo Windows server 2003
1	Servidor de firewall	Sistema operativo Linux
1	Sistema de adscripción de pacientes	Desarrollado en Visual Basic 6.0 con SQL server y cristal reports 2000
1	Sistema de registro de servicios médicos	Desarrollado en Visual Basic 6.0 con SQL server y cristal reports 2000
1	Sistema contable (CONPAQ),paquete de contabilidad	Desarrollado en Visual Fox pro
1	Sistema para el control de inventario general (ADMINPAQ)	Desarrollado en Visual Fox pro

6.4.3.2. Amenazas a los activos

- Los usuarios pueden causar daños al sistema o al equipo por descuido, por ignorancia o a propósito.

- Errores en la introducción de datos, borrado indebido de archivos o modificaciones no autorizadas.

- Errores en el diseño de aplicaciones.

- Sabotajes y robos de equipos o información.

- Difusión mal intencionada de información

- Programas maliciosos tales como: virus informático, gusanos informáticos, bomba lógica y programas espías (spyware).

- Intrusos que acceden a los datos o programas de los cuales no tienen acceso permitido (cracker, hacker, defacer, script kiddie o script boy, viruxer).

- Desastres naturales o domésticos (incendios, inundaciones, tormentas eléctricas, cortocircuitos, sobrecargas, terremotos).

- Personal interno del sistema, pueden causar daños por diferentes razones:
    1. Están descontentos.
    2. Son coaccionados.
    3. Pueden obtener beneficios personales

    .
- Desperfectos en los equipos informáticos, plantas generadoras, instalaciones eléctricas y todo lo referente a hardware.

- Señales de radar, la influencia de las señales o rayos de radar pueden inferir en el procesamiento electrónico de la información, sin embargo, solamente causa el daño si la señal que alcanza el equipo es de 5 Volts/Metro.

6.4.3.3. Vulnerabilidades del centro de cómputo

- El departamento de informática carece de políticas de seguridad informática.

- Poca preocupación por parte de los operadores informáticos con respecto a la protección del hardware.

- Las auditorias al departamento de informática son esporádicas.

- La infraestructura del sitio no está preparada para resistir inundaciones.

- No hay un lapso de tiempo establecido para cambiar las contraseñas.

- Solamente el 20% de las computadoras tienen su propia batería, el resto se conecta directamente a la corriente.

- Poco presupuesto económico designado al área informática.

- Utilizan sistemas operativos antiguos como Windows 98 y 2000.

- No utilizan programas para identificar vulnerabilidades.

- El respaldo de la información se realiza internamente en dos discos, pero no externamente, de forma que si ocurriera un desastre natural en el sitio donde están los servidores la información se perdería totalmente.

- No tienen un documento con medidas y procedimientos de neutralización y recuperación ante cualquier eventualidad que pueda paralizar total o parcialmente la actividad informática o funcionamiento del Hospital.

6.4.3.4. Análisis de las vulnerabilidades encontradas en el centro de cómputo

Se encontraron distintos tipos de vulnerabilidades (físicas, lógicas, administrativas) unas más graves que otras, no obstante todas pueden llegar a causar daños irreparables en los equipos y la información provocando pérdidas económicas, atrasos e inconvenientes a los pacientes y trabajadores de esta institución.

Muchas de estas vulnerabilidades son causadas quizás porque el presupuesto económico no es suficiente para resolver estas dificultades sin embargo, nos atrevemos a decir que la mayor causa es la falta de conciencia sobre la importancia de preservar la integridad, confiabilidad y disponibilidad de la información y la inexperiencia en el campo de la seguridad informática.

Toda institución tiene vulnerabilidades pueden ser mínimas o numerosas, es importante conocerlas y corregirlas mediante mecanismos de seguridad, capacitaciones al personal informático, planificación e implementación de planes de seguridad, que deben de ser de carácter recurrente porque la tecnología siempre esta cambiando , avanzando y junto con este continuo avance aparecen nuevas amenazas y riesgos a la información.

Para manejar el riesgo de cada amenaza la institución es responsable de elaborar un análisis de riesgo (probabilidad de ocurrencia, gravedad de la situación generada y costo de las medidas de prevención para actuar en consecuencia y asumir el riesgo en el caso que las medidas sean más costosas que las consecuencias de las amenazas).

6.4.4.1. Medidas preventivas de seguridad conforme a lo establecido por los controles A.5, A.7, A.9, A.10, A.11 Y A.12 que contiene la norma ISO 27001.

Control A.5 Política de seguridad

Es importante mencionar que las políticas de seguridad deben ser planificadas y documentadas por el jefe de informática y consensuado por los jefes administrativos, con amplia participación del área de sistemas. La administración es responsable de dar a conocer y hacer cumplir estas políticas de seguridad internamente, no obstante, presentamos una propuesta de políticas de seguridad para que sirva de ejemplo una vez que el departamento de informática del Hospital Militar “ADB” decida planificarlas y redactarlas.

Propuesta de políticas de seguridad

Políticas de seguridad para el área administrativa

- Gestionar auditorías internas en intervalos planificados de tiempo para garantizar la seguridad informática.
- Promover y realizar seminarios de formación y concienciación de todo lo referente a la seguridad informática.
- Actualizar planes de seguridad teniendo en cuenta los resultados de la monitorización y las revisiones.
- Implantar procedimientos, controles de detección y respuesta a incidentes de seguridad.
- Dar a conocer a los empleados reglas de seguridad.

Políticas de seguridad para el área informática

- Las computadoras deben usarse en un ambiente seguro.

- Las computadoras solo deben usarse para actividades de trabajo.

- No modificar hardware o software a menos que sea establecido por el departamento de informática.

- Cualquier problema en las computadoras o en la red debe reportarse inmediatamente para evitar perdida de información o interrupción de los servicios.

- Evitar dejar información sensible a disposición de personas no autorizadas.

- Bloquear la PC si se abandona.

Control A.7 Administración de recursos

De acuerdo con lo que establece este control se sugieren las siguientes acciones:

- Se debe tener un inventario de los activos físicos.
- Establecer una protección adecuada para estos activos.
- Debe definirse una clasificación de los activos relacionados con los sistemas de información, manteniendo un inventario actualizado que registre esos datos, y proporcionando a cada activo el nivel de protección adecuado en función de su criticidad.

Control A.9 Seguridad física y del entorno

Se sugieren las siguientes medidas de seguridad:

- Evitar accesos no autorizados, daños e interferencias contra el local.
- Cada equipo debe tener su propia batería.
- Alarmas contra incendios.
- Los fuegos Clase C involucran equipo eléctrico energizado, tales como aparatos eléctricos, interruptores, paneles, y tableros de electricidad. Por tanto se deben utilizar extinguidores de dióxido de carbono, químico seco ordinario, químico seco de uso múltiple o uno de halón. Nunca debe utilizarse agua en fuegos eléctricos ya que existe el riesgo de un choque o descarga eléctrica.
- Control de climatización (ventilación).

- Construcción de techos impermeables para evitar el paso de agua desde niveles superiores y acondicionar las puertas para contener el agua en caso de inundaciones.
- Documentación, planos de instalaciones, canales de comunicaciones y enlaces de radio.
- Realizar labores de mantenimiento y limpieza en los sitios donde se encuentran los equipos.
- Plantas de electricidad para asegurar la continuidad de las operaciones.
- El suministro eléctrico al centro de cómputo, y en particular la alimentación de los equipos, debe hacerse con condiciones especiales, como la utilización de una línea independiente del resto de la instalación para evitar interferencias.
- Los equipos ruidosos como las impresoras de impacto, equipos de aire acondicionado o equipos sujetos a gran vibración, deben estar en zonas donde tanto el ruido como la vibración se encuentren amortiguados.
- El sistema de iluminación debe ser apropiado para evitar reflejos en las pantallas, falta de luz en determinados puntos, y se evitará la incidencia directa del sol sobre los equipos.
- Las salas donde se encuentren los equipos deben de tener espacio disponible para la movilidad de los equipos, suelo móvil o suelo falso.
- Utilización de guardas de seguridad.
- Utilización de detectores de metal.
- Utilización de sistemas biométricos.

Control A.10 Administración de las comunicaciones y operaciones.

Según lo que establece este control se sugieren las siguientes medidas:

- Realizar respaldos (back-up) de la información y procesos de cómputo que se realizan en la dirección, conforme a parámetros preestablecidos.
- Llevar registros de fallas, problemas, soluciones, acciones desarrolladas, recuperaciones y trabajos realizados.
- Utilización de herramientas que detectan código malicioso como antivirus y antiespías.
- Actualización del sistema operativo.
- Redundancia: utilizar más de un mecanismo de seguridad.
- Uso de arquitecturas de red seguras: buen diseño de perímetros de red.
- Utilizar sistemas de búsqueda automática de vulnerabilidades, en este caso se propone **NESSUS.**
- Instalación de tecnologías protectoras cuidadosamente configuradas: cortafuegos(firewall), sistema de detección de intrusos(IDS).

Control A.11 Control de accesos

Con respecto al control de acceso a la red se deben tener las siguientes medidas:

- Como se ha mencionado en el control A.10 es indispensable tener cortafuegos.
- Autenticación de usuario para conexiones externas.
- Diagnóstico remoto y configuración de protección de puertos.
- Identificación de equipos en las redes
- Limitación del tiempo de conexión a internet.

Control de acceso al sistema operativo.

- Identificación de usuarios.
- Sistema de administración de contraseñas
- Selección de contraseñas “fuertes”, no transferirlas o escribirlas en archivos sin cifrar, evitar habilitar opciones de recordar las claves en el equipo; es importante cambiarlas frecuentemente.

Control de acceso de información y aplicaciones.

- Evitar el acceso no autorizado a la información contenida en los sistemas.
- Separar los sistemas que tienen un alto riesgo de ser comprometidos.

Control A.12 Adquisición de sistemas de información desarrollo y mantenimiento.

Se proponen las siguientes medidas:

- Evitar pérdidas, modificaciones o mal uso de los datos de usuario en las aplicaciones.
- Proteger la confidencialidad, autenticidad e integridad de la información.
- Debe contemplarse la seguridad en todas las etapas del ciclo de vida del software y las aplicaciones.

VII.CONCLUSIONES Y RECOMENDACIONES

Con la realización de este trabajo llegamos a las siguientes conclusiones:

1. La seguridad informática en el centro de cómputo del hospital militar presenta vulnerabilidades que ponen en riesgo la continuidad de la institución. Por tanto es imprescindible implantar y operar los controles propuestos en el plan de seguridad, sin embargo, la gestión de la seguridad informática no dará soluciones únicas ni totales.

   El control de las irregularidades solo puede lograrse con la intervención, apoyo del personal administrativo, concienciación, capacitación del personal informático y equipamiento robusto; es importante tomar en cuenta que estas acciones deben realizarse de forma recurrente debido a la continua evolución tecnológica.

2. El avance tecnológico permite grandes beneficios económicos a las organizaciones, pero también es campo potencial de errores y delitos informáticos.

3. La seguridad informática debe planificarse en todos sus niveles, en cualquier institución ya sea pública o privada no importando si es grande o pequeña.

4. La información es el activo más vulnerable de una institución, por tanto nunca se debe pensar que una institución no es blanco de ataques.

5. Una organización no es más segura por el hecho de esconder las vulnerabilidades que la afectan, sino porque estas se conozcan y corrijan, estableciendo las medidas de seguridad adecuadas.

Con el objetivo de mejorar el funcionamiento del centro de cómputo se recomiendan las siguientes acciones:

1. La gestión y la planificación de la seguridad informática debe ser estandarizada y documentada en manuales.

2. Elaborar planes de contingencia que ayude a tomar decisiones ante cualquier eventualidad que pueda paralizar total o parcialmente la actividad informática y el funcionamiento del Hospital.

3. El centro de cómputo debe ubicarse dentro de la institución a nivel de Staff, es decir, como una unidad independiente capaz de tomar sus propias decisiones, vinculada y comprometida con las exigencias propias de la institución.

VIII.BIBLIOGRAFÍA

Libros Consultados

- Cano, J. (2009).Computación forense, Descubriendo los delitos informáticos. México: Alfaomega Grupo Editor, S.A de C.V.

Fuentes Electrónicas

- Asobancaria. (2004). La informática forense y la banca. Obtenida el 17 de marzo de 2011,de http://www.asobancaria.com/upload/docs/docPag1993_1.pdf.

- Corletti, A. (2006). ISO-27001: Los controles (Parte I). Obtenida el 13 de octubre de 2010, de http://www.delitosinformaticos.com/11/2006/Seguridad-informática/iso-27001-los-controles-parte-i.

- Corletti, A. (2007).ISO-27001: Los controles (Parte II).Obtenida el 13 de octubre de 2010, de http://www.delitosinformaticos.com/01/2007/seguridad-informática/iso-27001-los-controles-parte-ii.

- Cano, J. (2004).Inseguridad informática: un concepto dual en seguridad informática. Obtenida el 12 de marzo de 2011, de http://www.virusprot.com/art47.html.

- Cano, J. (2006).Introducción a la informática forense, una disciplina técnico-legal. Obtenida el 27 de febrero de 2011, de http://www.acis.org.co/fileadmin/Revista_96/dos.pdf.

- Chávez, A. (2009).Seguridad informática. Obtenida el 14 de septiembre de 2010, de http://www.biblioteca.clacso.edu.ar/recursos/seguridad-informatica.pdf.

- Chacón, D. (2009).Norma ISO 27001 Informe. Obtenida el 05 de octubre de 2010, de http://djeffersec.site11.com/web_documents/ISO%2027001.pdf.

- Contreras, F. (2009).Herramientas de computación forense. Obtenida el 17 de marzo de 2011, de http://www.monografias.com /trabajos74/herramientas-computación-forense-control-digital.shtml.

- El nuevo diario. (2006). Hackers nicas obligan a aumentar seguridad informática. Obtenida el 14 de septiembre de 2010, de http://impreso.elnuevodiario.com.ni/2006/09/10/Seguridad-Informática/53830.

- ISO27000.es. (n.d).El portal de ISO 27001 en Español. Obtenida el 05 de noviembre de 2010, de http://www.ISO27000.ES.

- Scribd. (2010).ISO 27000.Obtenida el 05 de octubre de 2010, de http://es.scribd.com/doc/40168939/Doc-Iso27000-All.

- Scribd. (2010).Administración de centros de cómputo. Obtenida el 05 de noviembre de 2010, de http://es.scribd.com/doc/3081866/Administracion-de-Centros-de-Computo.

- Tenable Network Security. (2002).Nessus. Obtenida el 05 de noviembre de 2010 de http://www.nessus.org/products/nessus.

- Villalón, A. (2004).Códigos de buenas prácticas de seguridad. UNE-ISO/IEC 17799. Obtenida el 17 de septiembre de 2010, de http://wwww.shutdown.es/ISO177799.pdf.

- Wikibooks. (n.d).Seguridad informática. Obtenida el 14 de septiembre de 2010, de http://es.wikibooks.org/wiki/Seguridad_inform%C3A1tica/ Definici%C3%B3n.

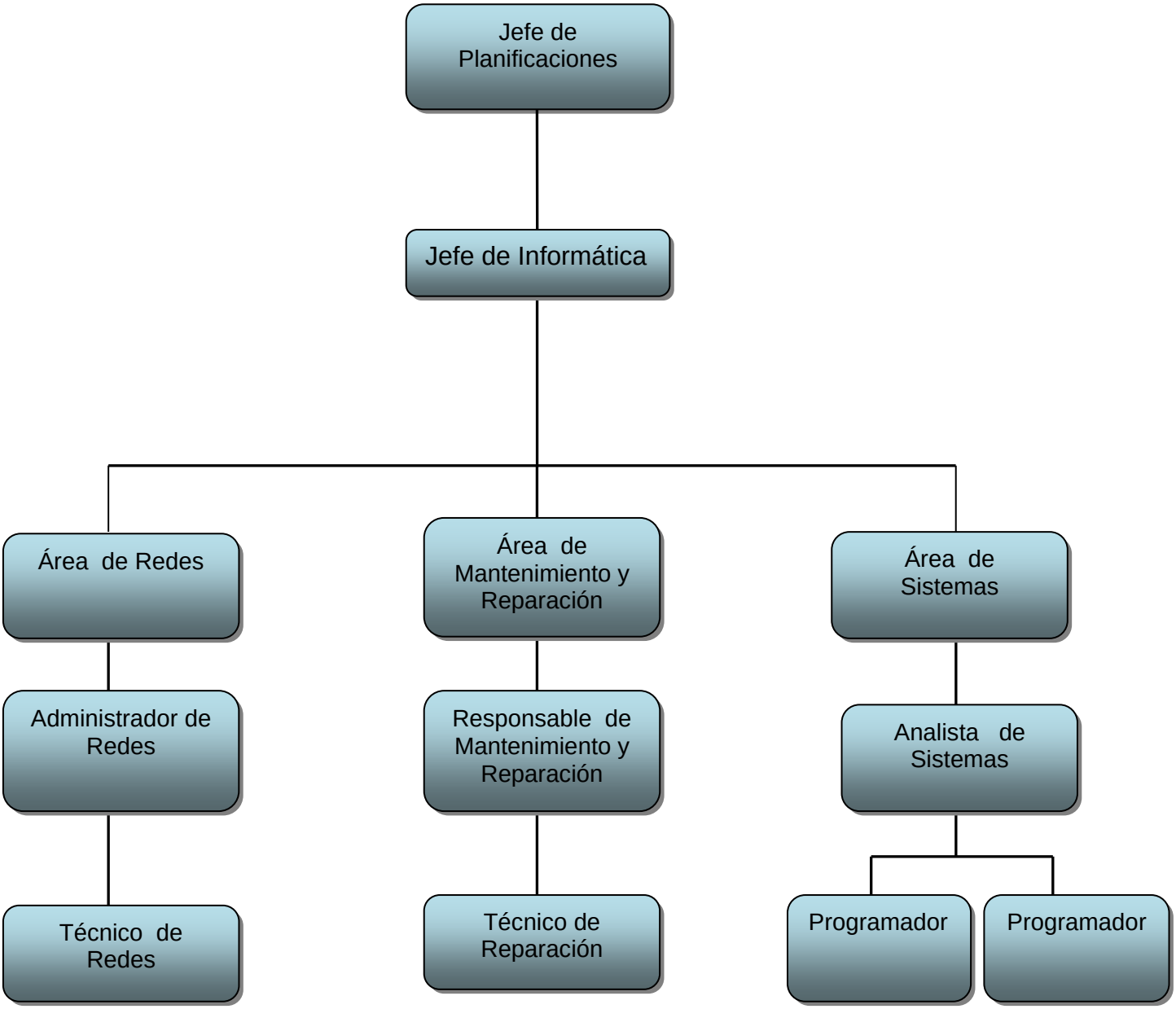
- Wikipedia. (n.d).Computación forense. Obtenida el 05 de noviembre de 2010, de http://es.wikipedia.org/wiki/C%C3%B3mputo_forense.

- Wikipedia. (n.d).Seguridad informática. Obtenida el 14 de septiembre de 2010, de http://es.wikipedia.org/wiki/seguridad_ inform%C3%A1tica.

- Wikipedia. (n.d). Nessus. Obtenida el 05 de noviembre de 2010, de http://es.wikipedia.org/wiki/Nessus**.**

IX.ANEXOS

9.1. Organigrama del Centro de Cómputo del Hospital Militar "ADB"



9.2. Modelo de entrevista

Cuestionario

Departamento de Informática

Hospital Militar Alejandro Dávila Bolaños

Nombre del entrevistado: _____

Cargo Actual: _____

Fecha: [/ /]

Hora: _____

Objetivo de la entrevista: Recopilar información para conocer el funcionamiento actual del centro de cómputo y determinar los elementos del análisis de riesgo.

1- **¿Cuáles son las funciones del centro de cómputo y que áreas dependen de este?**

2- **¿Cuántos servidores tiene el centro de cómputo?**

3- **¿Cuáles son las funciones de cada servidor?**

4- **¿En cuánto tiempo se bloquea el acceso a los servidores?**

5- **¿Cuántas computadoras, impresoras y conexiones de internet existen?**

6- ¿Qué sistema operativo tienen instalado las computadoras?

7- ¿Cuál es el nombre y la versión de los antivirus instalados en las computadoras?

8- ¿Cuántos sistemas de información poseen para controlar la gestión de la información en el hospital?

9- ¿Manejan un control de acceso a las bases de datos?

10-¿Respecto a las contraseñas, quiénes tienen acceso total al sistema?

11-¿Cada cuanto tiempo se cambian las contraseñas?

12-¿Existe alguna base de datos que controle la existencia de todas las contraseñas?

13-¿Cada cuanto tiempo se realiza el mantenimiento al hardware y software?

14-¿Qué tipo de amenazas se han presentado en el centro de cómputo?

15-¿Qué medidas se toman para prevenir la pérdida o sabotaje de la información?

16-¿Qué mecanismos utilizan para proteger tanto el hardware como el software?

17-¿Cómo está organizado el personal informático?

18-¿Existe alguna política de seguridad escrita?

19-¿El personal informático está plenamente consciente de la importancia que tiene la gestión de la seguridad informática?

20-¿Quiénes se encargan de planificar y gestionar la seguridad informática?

21-¿Cuál es la frecuencia con que se realizan las auditorias al centro de cómputo?

22-¿Cuáles serian las consecuencias si se perdiera información o si los sistemas fueran descontrolados a causa de un incidente?

23-¿Cuánto presupuesto se le asigna al departamento de informática?

X.GLOSARIO

1. **Bell_Lapadula**: El modelo de seguridad Bell-Lapadula, llamado así por sus creadores David Elliott Bell y Len LaPadula, consiste en dividir el permiso de acceso de los usuarios a la información en función de etiquetas de seguridad. Categorizándola en 4 niveles: no clasificado, confidencial, secreto y ultra secreto. Este modelo se centra en la confidencialidad y no en la integridad.

2. **Biba Model:** Sistema formal de transición de estados de política de seguridad que describe un juego de reglas de control de acceso diseñadas para asegurar que los datos no están contaminados. Supone una separación en niveles de integridad (análogo a los niveles de seguridad) con una relación ordenada. Los objetos son asignados a clases de integridad de acuerdo al daño que sufrirían si fueran modificados de manera inapropiada, y los usuarios asignados a clases de integridad basados en su veracidad.

3. **Backup:** Consiste en realizar copias de seguridad de la información, estas copias pueden realizarse de forma manual y periódica.

4. **Bomba Lógica:** Una bomba lógica es una parte de código insertada intencionalmente en un programa informático que permanece oculto hasta cumplirse una o más condiciones preprogramadas, en ese momento se ejecuta una acción maliciosa.

5. **Biométrico:** Corresponde a la biometría, la biometría es una tecnología de seguridad basada en el reconocimiento de una característica de seguridad y en el reconocimiento de una característica física e intransferible de las personas, como por ejemplo la huella digital.

6. **CEI:** Fundada en 1906, la CEI (Comisión Electrotécnica Internacional) es la principal organización del mundo para la preparación y publicación de normas internacionales para todas las tecnologías eléctricas, electrónicas y relacionadas. Éstos se conocen colectivamente como "electro tecnología". CEI ofrece una plataforma para las empresas, industrias y gobiernos de encuentro, discusión y desarrollo de las normas internacionales que requieren.

7. **Criptografía:** Ciencia que estudia la manera de cifrar y descifrar los mensajes para que resulte imposible conocer su contenido a los que no dispongan de unas claves determinadas. En informática el uso de la criptografía es muy habitual, utilizándose en comunicaciones y en el almacenamiento de ficheros. En comunicaciones, se altera mediante una clave secreta la información a transmitir, que circula cifrada hasta que llega al punto de destino, donde un sistema que conoce la clave de cifrado es capaz de descifrar la información y volverla inteligible.

8. **Cracker:** El término cracker (del inglés *crack*, romper), es cualquier persona que viola la seguridad de un sistema informático de forma similar a como lo haría un hacker, sólo que a diferencia de este último, el cracker realiza la intrusión con fines de beneficio personal o para hacer daño.

9. **Conficker:** También conocido como Downup Devian, Downandup y Kido, es un gusano informático que ataca el sistema operativo Microsoft Windows. El gusano explota una vulnerabilidad en el servicio Windows Server usado por Windows 2000, Windows XP, Windows Vista, Windows Server 2003, Windows Server 2008, y Windows 7.Cuando ha infectado un computador, Conficker desactiva varios servicios, como Windows Automatic Update, Windows Security Center, Windows Defender y Windows Error Reporting. Luego se contacta con un servidor, donde recibe instrucciones posteriores sobre propagarse, recolectar información personal o descargar malware adicional en el computador víctima. El gusano también se une a sí mismo a ciertos procesos tales como svchost.exe, explorer.exe y services.exe.

10. **DMZ:** El término se refiere normalmente como una zona de despeje por los profesionales de tecnología de la información. A veces se conoce como una red perimetral. El objetivo de una DMZ es añadir una capa adicional de seguridad a una organización de red de área local (LAN), un atacante externo sólo tiene acceso a los equipos en la zona de distensión, más que cualquier otra parte de la red.

11. **Defacer:** Este se dedica a explotar fallos en sitios web. Generalmente con ayuda de programas o bien, con sus conocimientos propios (puede llegar a cracker o hacker). Los defacer generalmente lo hacen por diversión o manifestar su inconformidad antes ciertas páginas, generalmente de gobierno. Aunque también solo intentar retar o intimidar a administradores.

12. **DISA:** Agencia de los Sistemas de Comunicación para la Defensa, organización militar de los EE.UU., responsable por la implementación y operación de los sistemas de información militar.

13. **Firewall:** Tecnología que busca desarrollar un control de acceso en el tráfico de red, con el fin de identificar qué paquetes pueden o no ingresar o salir del perímetro de la red de una organización.

14. **FDCC:** La Ley Federal Desktop Core Configuration(Escritorio federal básico de configuración) es una lista de seguridad de configuración recomendada por el Instituto Nacional de Estándares y Tecnología para el uso general microcomputadoras que están conectadas directamente a la red de una agencia del gobierno Estados Unidos .

15. **Hacker:** Del inglés hack, hachar. Término utilizado para llamar a una persona con grandes conocimientos en informática y telecomunicaciones y que los utiliza con un determinado objetivo. Este objetivo puede o no ser maligno o ilegal. La acción de usar sus conocimientos se denomina hacking o hackeo.

16. **HTML:** HyperText Markup Language (Lenguaje de Marcado de Hipertexto), es el lenguaje de marcado predominante para la elaboración de páginas web. Es usado para describir la estructura y el contenido en forma de texto, así como para complementar el texto con objetos tales como imágenes.

17. **IDS:** Los sistemas de detección de intrusos (Intrusion Detection System), es un mecanismo de seguridad propio del mundo cliente/servidor, pues actúa como un monitor de tráfico de red, descubriendo y analizando el contenido de los paquetes que ingresan a la organización.

18. **Javascript:** Es un lenguaje de scripting basado en objetos utilizado para acceder a objetos en aplicaciones. Principalmente, se utiliza integrado en un navegador web permitiendo el desarrollo de interfaces de usuario mejoradas y páginas web dinámica.

19. **LaTeX:** Es un sistema de composición de textos, orientado especialmente a la creación de libros, documentos científicos y técnicos que contengan fórmulas matemáticas. LaTeX está formado por un gran conjunto de macros de TeX, con la intención de facilitar el uso del lenguaje de composición tipográfica.

20. **Malware:** Del inglés (malicious software), también llamado badware, software malicioso o software malintencionado es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora sin el consentimiento de su propietario. El término malware es muy utilizado por profesionales de la informática para referirse a una variedad de software hostil, intrusivo o molesto.

21. **Mainframe:** Una computadora central o mainframe es una computadora grande, potente y costosa usada principalmente por una gran compañía para el procesamiento de una gran cantidad de datos.

22. **Mac:** En redes de ordenadores, la dirección MAC (siglas en inglés de Media Access Control o control de acceso al medio) es un identificador de 48 bits (6 bloques hexadecimales) que corresponde de forma única a una tarjeta o dispositivo de red. Se conoce también como la dirección física. Es única para cada dispositivo

23. **Nmap:** Es un programa de código abierto que sirve para efectuar rastreo de puertos escrito originalmente por Gordon Lyon (más conocido por su alias Fyodor Vaskovich). Se usa para evaluar la seguridad de sistemas informáticos, así como para descubrir servicios o servidores en una red informática.

24. **NSA:**(National Security Agency - Agencia Nacional de Seguridad). Agencia estadounidense dedicada especialmente a la seguridad informática.

25. **Proxy:** Un proxy, en una red informática, es un programa o dispositivo que realiza una acción en representación de otro, por ejemplo si una hipotética máquina a solicita un recurso a una c, lo hará mediante una petición a b; C entonces no sabrá que la petición procedió originalmente de a. Su finalidad más habitual es la de servidor proxy, que sirve para permitir el acceso a Internet a todos los equipos de una organización cuando sólo se puede disponer de un único equipo conectado, esto es, una única dirección IP.

26. **Protocolo:** Conjunto de estándares que controlan la secuencia de mensajes que ocurren durante una comunicación entre entidades que forman una red.

27. **Polimorfismo:** En general, polimorfismo describe múltiples y posibles estados de una única propiedad. En computación es también una técnica utilizada por virus informáticos y gusanos para modificar partes de su código dificultando su detección.

28. **P2P:** Una red peer to peer o red de pares o red entre iguales o red entre pares o red punto a punto (P2P, por sus siglas en inglés) es una red de computadoras en la que todos o algunos aspectos funcionan sin clientes ni servidores fijos, sino una serie de nodos que se comportan como iguales entre sí. Es decir, actúan simultáneamente como clientes y servidores respecto a los demás nodos de la red. Las redes P2P permiten el intercambio directo de información, en cualquier formato, entre los ordenadores interconectados.

29. **PCI**: Security Standards Council (El consejo de normas de seguridad) Es un organismo de normas de seguridad de datos, en el sector de tarjetas de pago, requisitos de seguridad en las transacciones de números de identificación personal y normas de seguridad de datos de aplicación de pagos.

30. **Plugins:** Programa que puede anexarse a otro para aumentar sus funcionalidades (generalmente sin afectar otras funciones ni afectar la aplicación principal). No se trata de un parche ni de una actualización, es un módulo aparte que se incluye opcionalmente en una aplicación.

31. **Spyware:** Es un programa, que funciona dentro de la categoría malware, que se instala furtivamente en un ordenador para recopilar información sobre las actividades realizadas en éste. La función más común que tienen estos programas es la de recopilar información sobre el usuario y distribuirlo a empresas publicitarias u otras organizaciones interesadas.

32. **TCP/IP:** Es un conjunto de protocolos. La sigla TCP/IP significa "Protocolo de control de transmisión/Protocolo de Internet" .Proviene de los nombres de dos protocolos importantes del conjunto de protocolos, es decir, del protocolo TCP y del protocolo IP.

33. **Viruxer:** Alguien que produce un código de auto replicación que incluye una carga peligrosa.

34. **XML:** Son las siglas de Extensible Markup Language, una especificación/lenguaje de programación, diseñado especialmente para los documentos de la web. Permite que los diseñadores creen sus propias etiquetas, permitiendo la definición, transmisión, validación e interpretación de datos entre aplicaciones y entre organizaciones.