UNIVERSIDAD AUTONOMA DE CHIAPAS

UNACH

Auditoría en informática asistida por tecnología con dictamen y sugerencias

Carmen Carolina Ortega Hernández

Facultad de Contaduría Pública,
Campus IV - Tapachula

Auditoría en Informática, asistida por tecnología, con dictamen y sugerencias
Carmen Carolina Ortega Hernández

Carmen Carolina Ortega Hernández

*

AUDITORÍA EN INFORMÁTICA ASISTIDA POR TECNOLOGÍA

CON DICTAMEN Y SUGERENCIAS

*

PRIMERA EDICIÓN

*

Primera edición

Noviembre 2014

Auditoría en Informática, asistida por tecnología, con dictamen y sugerencias.

FACULTAD DE CONTADURÍA, CAMPUS IV-TAPACHULA

UNIVERSIDAD AUTÓNOMA DE CHIAPAS

ISBN: 978-607-8304-21-9

Revisión técnica:

Academia de Informática. Programa de Licenciatura en Sistemas Computacionales. Facultad de Contaduría, Campus IV. Tapachula. UNACH

Dr. David Ristori Cueto y Dra. Alma Leslie León Ayala. Docentes de la Facultad de Contaduría, Campus IV. Tapachula. UNACH.

DES: Ciencias Administrativas y Contables

Dr. Juan Carlos Román Fuentes

Coordinador Editorial de la DES

Diseño de portada: Víctor M. Villalobos H.

Apoyo editorial: José Manuel Villar

Hecho e Impreso en México.

DIRECTORIO

Mtro. Jaime Valls Esponda
Rector

Mtro. Hugo Armando Aguilar Aguilar
Secretario General

Mtro. Luis Iván Camacho Morales
Secretario Académico

Mtro. Miguel Ángel Cigarroa Torres
Secretario Administrativo

Mtro. Juan Carlos Rodríguez Guillén
Director General de Planeación

Dr. Lorenzo Franco Escamirosa Montalvo
Director General de Investigación y Posgrado

Lic. Víctor Fabián Rumaya Farrera
Director General de Extensión Universitaria

DES: Ciencias Administrativas y Contables:

Dr. Felipe de Jesús Gamboa García
Director Facultad de Contaduría y Administración, Campus I

Mtro. Enrique Yasusi Barroso Yoshikawa
Director Facultad de Contaduría, Campus IV

Mtra. Mónica Juárez Ibarias
Directora Facultad de Ciencias de la Administración, Campus IV

C.P. Andrés Morales Martínez
Director de la Escuela de Contaduría y Administración, Campus VII

Mtro. Héctor Antonio Gordillo Palacios
Encargado de la Facultad de Ciencias Administrativas, Campus VIII

Mtro. Hernán Hernández Marroquín
Director de la Escuela de Ciencias Administrativas, Campus IX-Tonalá

Mtra. Hilda García Castillo
Encargada de la Coordinación de la Escuela de Ciencias Administrativas, Campus IX-Arriaga

Prólogo

Las tecnologías de la información y la comunicación (TIC's) observan un vorágine desarrollo, y por ello paulatinamente se incrustan en forma transversal en todos los ámbitos de la vida, abarcando aspectos familiares, laborales y escolares, por citar algunos. Por otro lado, los sistemas operativos, las aplicaciones y los dispositivos cada vez tienen una menor vida útil, en el sentido, de que poco tiempo después de haberlos adquiridos se encuentran en el mercado otros más avanzados, que reducen tiempos y esfuerzos requeridos para la obtención de los propósitos.

A lo anterior, surge el cuestionamiento ¿qué tan segura es la tecnología adoptada?, ¿es adecuada a las necesidades organizacionales?, ¿los equipos adquiridos están siendo subutilizados?, ¿el uso de las TIC's se encuentran dentro del marco de legalidad? Estas interrogantes, provocan la reflexión y la revisión, desde una perspectiva profesional sobre las diversas opciones para dictaminarlo; de esta necesidad surge la Auditoria en Informática o Auditoria en Sistemas Computacionales, dedicada a la revisión detallada de estos aspectos.

En este contexto, esta propuesta bibliográfica transita por los conceptos de los diferentes tipos de auditoría como son: *web*, *software*, bases de datos, redes y *hardware*, también recopila las principales disposiciones legales aplicables en el país, que constituyen el marco normativo, en materia de TIC's, puntualizando casos prácticos en torno al fenómeno informático. Presenta las mejores opciones de programas de diagnóstico para la auditoría en los sistemas computacionales que se distribuyen actualmente e incluye un cuestionario para recolección de datos que miden el rendimiento de la función informática. Al final, presenta una novedosa metodología para crear un Sistema Gerencial que de manera accesible permite generar el dictamen de la revisión practicada y las sugerencias correspondientes.

La autora de este libro, apasionada estudiosa de esta área, pone a disposición de los lectores, estudiantes, docentes y profesionales interesados en el tema, esta interesante alternativa, creativa y original, entorno a la auditoria asistida por la tecnología.

Este libro viene a aportar un eslabón en la cadena cognitiva que impulsa la generación y aplicación de conocimientos en la disciplina informática y en el ámbito del Desarrollo Organizacional.

Dr. David Ristori Cueto

Introducción

Hoy más que nunca, resulta necesario que las organizaciones reconozcan la importancia de realizar una auditoría en Sistemas Computacionales y/o Informática, en las áreas de procesamiento electrónico para evaluar el control que se tiene implementado y el grado de probabilidades de que ocurra un suceso no deseado, con la finalidad de planear nuevas acciones o modificar las existentes, en una adecuada toma de decisiones. Pero, cuando se piensa en una Auditoría, acuden a la mente aspectos técnicos y administrativos a supervisar, es por ello que esta actividad se considera laboriosa, donde la experiencia y la habilidad juegan un papel importante, al momento de elegir las estrategias que permitan recolectar, analizar y evaluar la información de una manera eficiente y eficaz.

En base a esta necesidad, el presente libro ofrece una nueva alternativa de Auditoría asistida por la tecnología; basándose en el diseño de una metodología para el desarrollo de un Sistema Gerencial de Evaluación, que emplea como datos de entrada los reportes emitidos por los programas de diagnóstico para computadoras y redes de comunicación que existen actualmente, y los resultados generados por un cuestionario previamente automatizado; para generar de forma imparcial y consistente el Dictamen y las Sugerencias, a partir de los resultados auditados.

Para diseñar un *software* de auditoría en informática es necesario definir la metodología de trabajo (Cap. V); pero antes de abordar el tema principal, se brinda al lector información relacionada al área de estudio; por ejemplo, existen diversos tipos de auditorías especializadas, entre las cuales destacan: *web, software*, bases de datos, redes y *hardware* (Cap. I), que deben considerarse al momento de definir el alcance del trabajo; así también, en el país se tiene un marco jurídico extenso formado principalmente por las siguientes ordenamientos: Código Penal, Ley Federal de Telecomunicaciones, Ley Federal del Derecho de Autor, Ley Federal de la Propiedad Industrial, Ley Federal de Protección al Consumidor, Ley de Protección de Datos Personales en Posesión de Particulares (Cap. II), indispensables para describir los derechos y obligaciones de los usuarios, así como las violaciones y sanciones que pueden derivarse por el incorrecto uso de los recursos.

En el proceso de recolección de datos, se consideran programas de diagnóstico que generan reportes en las categorías de *software, hardware*, dispositivos, base de datos, redes e *internet*; son tan eficientes que pueden presentar en segundos, un inventario por equipo, con la relación de programas instalados, sistema de arranque y las licencias de los mismos;

así también, ofrecen un informe detallado con las características del microprocesador, memoria, discos lógicos, unidades extraíbles, puertos de comunicación, protocolos de red y direcciones IP, entre otras, el cual puede ser emitido en formato de texto, PDF, HTML, o exportado a una base de datos; y aunque existe una gran variedad, destacan: *WinAudit, OpenAudit, FreshDiagnose, Lansweeper, Total Network Inventory, Softkey, TAW, WhatWeb, XRumer, Watobo, Secure Auditor, ApexSQL, NESSUS, NMAP y WhireShark* (Cap. III).

Otro aspecto importante son las vulnerabilidades y amenazas que se presentan cuando se logra una simbiosis entre el recurso humano y el recurso tecnológico en el desarrollo de las actividades cotidianas; una forma de afrontarlas es la elaboración de una Evaluación del Riesgo, la definición de Actividades de control preventivo, de detección y de corrección, y la aplicación de Políticas de Seguridad; y si resulta de interés enfocarse en la medición de acciones de control, pueden aplicarse cuestionarios en el área de tecnología, recursos humanos, gestión administrativa, infraestructura y recursos materiales (Cap. IV); generando concentrados de datos, para su correspondiente interpretación de resultados.

A partir de lo anterior puede observarse, que la auditoría en informática es un proceso joven que ha ido creciendo en forma paralela al desarrollo de nuevas tecnologías y la dependencia de éstas en el ámbito organizacional. Con estas consideraciones, en esta edición se ofrece un contexto actualizado de los tópicos descritos, que cubren tanto requerimientos de estudio de universitarios como intereses laborales de profesionales en la materia.

Un libro no solamente contiene palabras, entre cada línea hay inspiración y regocijo, es por ello que agradezco a mi esposo Alonso Cano Meléndez, por su motivación en la creación del proyecto; a mis adorados hijos Gilberto y Carolina por su comprensión e impulso por alcanzar la meta, permitiendo que las ideas nacieran desbordadas, esperando a ser tomadas en cuenta cuando el día terminaba; a mis amados padres Gloria Zoila Hernández Lemus y Pablo Ortega Cortés que me enseñaron a saborear intensamente cada línea, hoy gracias a todos ellos, puedo asegurar "que se aprende a leer cuando se empieza a escribir".

Asimismo, mi reconocimiento personal al Dr. David Ristori Cueto, por el prólogo y revisión de la obra y por las palabras de aliento, cuando el ánimo disminuía ante el camino sinuoso, que significa una obra como ésta.

L.I. Carmen Carolina Ortega Hernández

Índice

Capítulo III. Programas Diagnósticos para la Auditoría en Informática

Capítulo IV. Riesgo y Control

Capítulo V. Metodología para diseñar Software de Auditoría en Informática

Índice de Figuras

Acerca de la Autora

Carmen Carolina Ortega Hernández es oriunda de Tapachula, Chiapas, egresada de la Licenciatura en Informática del Instituto Tecnológico de Tapachula y de la Maestría en Ciencias Computacionales en la Universidad Autónoma de Guadalajara.

La Asociación Nacional de Facultades y Escuelas de Contaduría y Administración (ANFECA) la acredita como académica certificada en Informática Administrativa.

El Consejo para la Acreditación de la Educación Superior A.C. (COPAES) la reconoce como miembro evaluador, por su participación activa en el Consejo de Acreditación en Informática y Computación A.C. (CONAIC), en comisiones técnicas para la evaluación de los programas de estudio de nivel superior en instituciones públicas y privadas a nivel nacional.

Se ha desempeñado como docente de la Universidad Autónoma de Chiapas, en las Licenciaturas en Contaduría y en Sistemas Computacionales, por más de 17 años.

Es pionera y precursora del proceso de Acreditación del Programa de Estudios de la Licenciatura en Sistemas Computacionales de la Facultad de Contaduría, Campus IV, de la Universidad Autónoma de Chiapas, ante el organismo acreditador.

Con espíritu constructivo ha participado en la dirección de tesis, dirección y elaboración de revistas de tecnologías, congresos, cursos, talleres y diplomados; asimismo, ha desempeñado responsablemente la Coordinación del programa educativo, del programa de egresados y del programa de acreditación de la Licenciatura en Sistemas Computacionales.

En forma alterna y con la misma responsabilidad y entrega ha participado en Instituciones educativas del nivel medio Superior y Básico.

CAPÍTULO I

AUDITORÍA EN INFORMÁTICA

Auditoría *WEB*

Auditoría de *Software*

Auditoría de Bases de Datos

Auditoría de Redes

Auditoría de *Hardware*

1.1. Objetivo de la Auditoría

Las instituciones que contratan los servicios de un auditor o que someten sus procedimientos a una evaluación, lo hacen con el objetivo de revisar el funcionamiento de sus controles internos, ya que en muchas ocasiones las amenazas y vulnerabilidades están presentes y dejan de ser percibidas, hasta por el mismo personal que labora diariamente, esto ocurre cuando se realizan actividades que no están debidamente controladas y solo ocasionan que aumente la probabilidad de que ocurran sucesos no deseados, donde la única forma de abatirlos es, primero detectarlos y después aplicar las medidas preventivas y/o correctivas correspondientes.

Existen muchos tipos de Auditoría (*ver. Fig. 1*) y todas tienen el mismo objetivo, el cual consiste en la supervisión de los procedimientos y procesos a través de medios tangibles, con el fin de evaluar su gestión, control y nivel de seguridad, para ofrecer cursos alternativos de acción y un dictamen imparcial de la situación actual; pero, existe una diferencia que distingue una de otra, ésta se basa en el área de aplicación.

Figura 1. Tipos de Auditoría

Fuente: [elaboración propia]

Por ejemplo la auditoría financiera controla la eficiencia de los estados financieros; la auditoría operacional, la eficiencia de los procedimientos organizacionales; la auditoría fiscal, la eficiencia en el cumplimiento de las normas fiscales; y de esta manera pueden citarse cada una de ellas, pero el enfoque central de este libro se centra, en aquella que se encarga de controlar la eficiencia en el procesamiento de información a través de los sistemas automatizados y que se denomina: Auditoría en Informática.

1.2. Auditoría en Informática y Auditoría en Sistemas

Hoy en día, la tecnología juega un papel muy importante al momento de salvaguardar los activos de una empresa, es por ello que los directivos no dudan en someter sus controles y procesos a una auditoría, ya que el éxito de sus operaciones depende en gran medida de la gestión de su información, misma que recorre todos los departamentos como un recurso vital; es por ello que la seguridad, integridad, confiabilidad, calidad y normatividad de los datos deben de ser examinadas periódicamente, pero se encuentran con la interrogante de ¿cuál solicitar?, pues sobresalen dos:

"Auditoría en Informática (AI) o Auditoría en Sistemas (AS)"

Para realizar la diferencia entre las dos, a continuación se define cada una de ellas, a través de la opinión de dos autores, iniciando con Auditoría en Informática: "*es la revisión y evaluación de los controles, sistemas, procedimientos de informática; de los equipos de cómputo, su utilización, eficiencia y seguridad, de la organización que participan en el procesamiento de la información, a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones" (Echenique, 2000:16)* y Auditoría en Sistemas: "*es la parte de la auditoría interna que se encarga de llevar a cabo la evaluación de normas, controles, técnicas y procedimientos que se tienen establecidos en una empresa para lograr confiabilidad, oportunidad, seguridad y confidencialidad de la información que se procesa a través de computadores; es decir, en estas evaluaciones se están involucrando tanto los elementos técnicos como humanos que intervienen en el proceso de la información". (Eurípides Rojas citado en Tamayo Alzate, 2001).*

Después de analizar los conceptos anteriores, es probable que exista alguna confusión, por ello, para disipar cualquier duda, puede concluirse que la AI abarca a la AS, es decir, la primera ofrece una proyección generalizada, que incluye el análisis de los recursos humanos, de los procedimientos operativos y administrativos, de la infraestructura y mobiliario, y finalmente de la tecnología y comunicaciones que se involucran en el proceso; a diferencia de la segunda que solo contempla el último rubro citado, pero que en ningún momento deja de ser menos importante ya que realiza un examen exhaustivo de los programas de aplicación o de gestión instalados en los equipos, de la comunicación interna y externa entre ellos, de la confiablidad y seguridad de sus transacciones, de la existencia de documentación y del rendimiento de sus dispositivos e interfaces, entre otros.

Ahora, teniendo el conocimiento de cada una y considerando la necesidad que tienen las organizaciones de un examen completo y meticuloso que detecte los riesgos para tomar medidas preventivas o correctivas, se han propuesto nuevos términos que incluyan las características de las dos. Algunos autores llaman a esta fusión, Auditoría en Sistemas Computacionales (ASC), Auditoría en Sistemas de Información (ASI) o Auditoría en Tecnologías de Información (ATI), las tres con el mismo objetivo y alcance.

Para conocer su complejidad y alcance a continuación se ofrece la definición de Auditoria en Sistemas Computacionales, como *"la revisión técnica, especializada y exhaustiva que se realiza a los sistemas computacionales, software e información utilizados en una empresa, sean individuales, compartidos y/o redes, así como a sus instalaciones, telecomunicaciones, mobiliario, equipo periféricos y demás componentes. Dicha revisión se realiza de igual manera a la gestión informática, el aprovechamiento de sus recursos, las medidas de seguridad y los bienes de consumo para el funcionamiento del centro de cómputo. El propósito fundamental es evaluar el uso adecuado de los sistemas para el correcto ingreso de los datos, el procesamiento adecuado de la información y la emisión oportuna de sus resultados en la institución, incluyendo la evaluación en el cumplimiento de las funciones, actividades y operaciones de funcionarios, empleados y usuarios involucrados con los servicios que proporcionan los sistemas computacionales en la empresa"; citado en (Muñoz Razo, 2002:23).*

1.2.1. El futuro de la Auditoría en Informática

La tecnología sigue evolucionado a pasos agigantados, se actualizan técnicas y herramientas que ofrecen un control más eficiente, atractivo y de fácil de manejo, los antiguos mecanismos inmediatamente son remplazados y en muchas ocasiones sin realizar un análisis de fortalezas y debilidades se promueve el cambio de ellas, los controles ya no se limitan a un entorno interno, el uso de la *web* ofrece nuevas alternativas de transacciones, en donde la información digital transciende fronteras a través del *internet*, el procesamiento de la información asciende a un nivel más alto en donde se presentarán amenazas que antes se desconocían y el auditor deberá estar consciente de cada una de ellas, para seguir presentando resultados útiles.

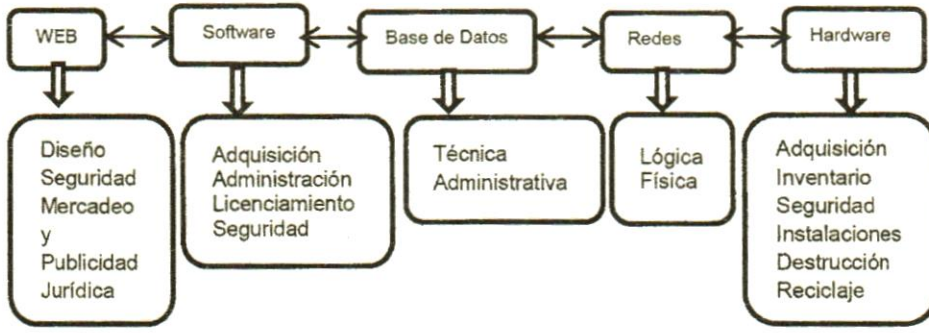
En algunos años, no dudando de la creatividad del ser humano, se esperan nuevas terminologías, las cuales serán apropiadas, porque cubrirán más necesidades, algunas incluirán en su nombre el área de especialización que indicará la profundidad de su alcance, pero todas se basarán en un solo principio: la Informática.

1.3. Auditorías Especializadas en el Área Informática

Cuando se inicia una auditoría es necesario conocer el entorno del negocio, para interpretar su funcionamiento; ésta etapa es reconocida como investigación preliminar y se basa principalmente en la revisión documental de los siguientes documentos: se inicia con el proyecto de trabajo, que contiene los objetivos, estrategias, acciones y actividades que se llevan a cabo; después con el manual de funciones y roles para conocer la distribución de las actividades por personas; y finalmente las políticas de seguridad para saber, qué elementos tienen sujetos a protección. El proceso de evaluación inicia, desde el momento en que se comprueba la existencia de los documentos anteriores, pero también, es importante considerar si existe una correcta difusión, actualización y aplicación de los mismos.

Después de tener un bosquejo general de las necesidades de la organización se puede continuar con el desarrollo del programa de auditoría enfocado a áreas especializadas para un mejor impacto y rendimiento, entre las cuales, figuran: *software, hardware*, bases de datos, *web* y redes (ver Fig.2), y asimismo sus puntos más relevantes.

Figura 2. Tipos de Auditoría Especializadas en el Área de Informática



Fuente: [elaboración propia]

1.3.1. Auditoría *Web*

El futuro de las transacciones es *internet* y los directivos han comprendido esta realidad, orientando sus estrategias organizacionales a un nuevo mercado, que exige más controles y presenta mayores retos. El proyecto se realiza en tres etapas, la primera se basa en el diseño, desarrollo y mantenimiento del sitio *web*, el cual puede estar a cargo por personal interno del área de informática o contratar personal externo acreditado, la segunda mide resultados en relación a los clientes y los ingresos, los cuales no siempre son redituables en el tiempo que se espera, o en su defecto nunca se recupera la inversión realizada, no es necesario llegar a este punto, para iniciar la última etapa, que consiste en contratar a un experto en auditoría *web* que evalúe los aspectos técnicos, legales, fiscales, logísticos, de mercadeo y distribución, que ofrecen calidad, confiabilidad, disponibilidad y seguridad a las páginas *web*, con la finalidad de detectar errores y ofrecer alternativas de solución. Por su extenso alcance, es necesario identificar áreas específicas:

1.3.1.1. Auditoría Diseño *Web*

Actualmente existen muchas herramientas que permiten diseñar páginas *web* empresariales en minutos, un ejemplo podría ser: *Dreamweaver, Fireworks, Logo Creator y Filezilla*; asimismo, existen lenguajes como html, xml o xslt entre otros, si lo que se desea es programar; ambas alternativas son correctas, pero antes de decidir cuál elegir, es necesario considerar el presupuesto y el objetivo, pues no se busca crear una página "fantasma" que nadie visite por no estar accesible, disponible o mal diseñada.

Para detectar las vulnerabilidades en el diseño, desarrollo e implementación de la página, dominio y alojamiento (*hosting*), es necesario realizar una evaluación técnica que contemple el control de visitas, la accesibilidad de los contenidos que incluyen evaluar acentos, textos de referencia, de imágenes, animaciones, gráficas, tablas e hipervínculos, encabezados y títulos, el nombre de dominio (20 letras/espacios aprox.), el nombre del título (60 letras/espacios aprox.), la capacidad de hospedaje, ancho de banda y correos electrónicos institucionales. La *World Wide Web Consortium* denominada por sus siglas en inglés en *W3C,* es un organismo acreditador a nivel internacional reconocido ampliamente en México, para regular los niveles de usabilidad y accesibilidad de la tecnología *web* y *TawOnClick*, es una aplicación de apoyo.

1.3.1.2. Auditoría Seguridad *Web*

Existen miles de clientes que se resisten al cambio, por la desconfianza que tienen al introducir sus datos personales en una página *web*, y sin tener el conocimiento pleno de la situación no están alejados ante la realidad que implica estar en el último nivel de un sistema informático; la capa de seguridad de una aplicación *web* se vuelve más vulnerable por los ataques al código con el fin de robar información entre los más comunes se encuentran las inyecciones por lenguaje estructurado de consultas, denominado por sus siglas en inglés SQL, asimismo el robo de *cookies* y cuentas de usuario por inyecciones de código conocido como *Cross Site Scripting* y denominado por sus siglas como: XSS.

Una forma de detectar vulnerabilidades es el análisis del código fuente mediante la auto inclusión controlada de etiquetas *<script>* y *<frame>* para filtrar código malicioso de una página a otra página local o el envío de rutas a través de URL, acrónimo de *Uniform Resource Locator*, asimismo por medio de *cookies* o cabeceras del Protocolo de transferencia de hipertexto denominado HTTP por sus siglas en inglés, para entrar a páginas sin abrir sesiones.

Una fortaleza para evitar los registros automáticos es incluir en el formulario los *CAPTCHA* reconocido de esta manera por su acrónimo *Completely Automated Public Turing test to tell Computers and Humans Apart,* que actualmente se pueden conectar a servicios gratuitos de sistemas de validación humana con modalidad tecleo y de audio; además existen aplicaciones de apoyo, como: *Pipper, WhatWeb, XRumer.*

1.3.1.3. Auditoría Mercadeo y publicidad *Web*

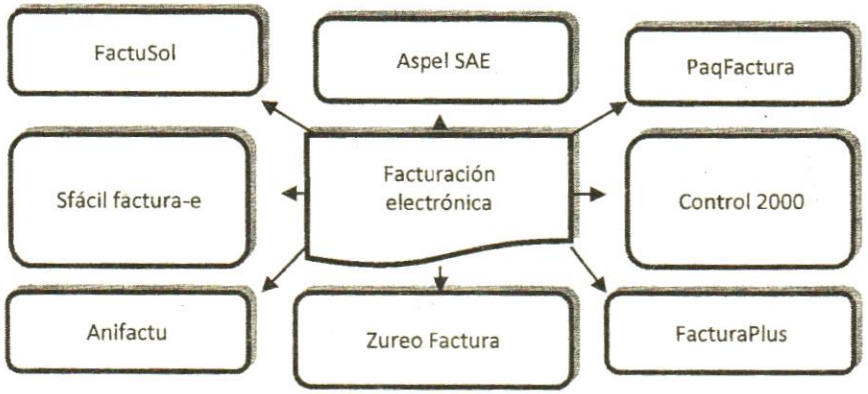
El grado de integración que tiene la página *web* con el plan promocional de la organización es muy importante, existen datos de gran interés que se deben evaluar, como la presencia, el logotipo, teléfonos de contacto, domicilio fiscal, el origen y la frecuencia de las visitas, los servicios o productos que más interesan a los usuarios, el historial de los enlaces de otros sitios, la prioridad que tienen las palabras claves en los buscadores y mensajes de advertencia cuando su publicidad contenga información que afecte a niños, ancianos o enfermos.

Una buena estrategia de mercadotecnia sería presentar atractivamente la información sobre el producto o servicio, sin crear una publicidad engañosa o desleal.

1.3.1.4. Auditoría Fiscal *Web*

La autoridad fiscal del país Servicio de Administración Tributaria denominada SAT, exhorta y obliga a las empresas mexicanas registradas, a realizar su facturación de forma electrónica, esto incorpora nuevas especificaciones al trabajo de auditoría, en donde por su naturaleza digital, deberán ser examinadas las licencias de los programas de aplicación *(ver Fig.3),* el control de procesamiento automático de subtotales y totales, las consultas del catálogo de productos, la impresión en formatos de documentos portátiles que por sus siglas en inglés se les conoce como PDF y la cancelación de facturas, incluyendo el mismo proceso para los recibos de honorarios y arrendamientos, si éstos existen.

Figura 3. Programas Contables para el Procesamiento de Facturas Electrónicas



Fuente: [elaboración propia]

Con base al artículo 29-A del (Código Fiscal de la Federación, 2011), los datos que deben estar presentes en los comprobantes fiscales son: registro federal de contribuyentes o mejor conocido como RFC, domicilio fiscal de la empresa, número de folio, sello digital, lugar y fecha de expedición, código de barra, logotipos, descripción de productos o servicios, importes, impuestos trasladados, importe total en número y letra, RFC del destinatario del comprobante y número de la cuenta o de la tarjeta del beneficiario del comprobante y la firma electrónica, comprobando la fiabilidad de la misma en base a los términos del artículo 97 del (Código de Comercio, 2014), y en el caso de mercancías de importación agregar el número y fecha del documento aduanero.

1.3.1.5. Auditoría Jurídica *Web*

Cuando se refiere al uso libre del *internet*, se alude a la libertad de usar la infraestructura en Telecomunicaciones que tiene el país; pero, sin incluir la creación de páginas, el alojamiento de las mismas en los servidores, el diseño del programas y la administración de datos personales; debido a que éstos aspectos son regulados por normas y leyes para mantener la legalidad del sitio y la protección de los proveedores y consumidores en un ambiente virtual.

A continuación se presenta información de cada apartado, que debe estar incluida en la lista de evaluación:

a) Registro de dirección IP y Dominio

Para garantizar que las direcciones IP denominado de esta manera por sus siglas en inglés, que significa "*Internet Protocolo*" y que los dominios sean únicos, se deben consultar a los organismos responsables de la administración de DNS a nivel internacional y nacional, a través de las páginas del ICANN (*Internet Corporation for Assigned Names and Numbers*) y de la NIC (*Networks Information Center*, México). *(Ver Fig.4).*

Figura 4 . Logotipos del ICANN y NIC México

Fuente: [Elaboración propia, basado en logotipos tomados del (ICANN) y (NIC México)

b) La legalidad de los contenidos

Se relaciona con los derechos de autor o propiedad intelectual, es por eso, que la autenticidad de las obras se garantiza con la existencia del registro de logotipos, marcas, patentes, imágenes, textos y código del programa, en el IMPI (Instituto Mexicano de la Propiedad Industrial) y en el OMPI (Organismo Mundial de la Propiedad Intelectual) *(Ver Fig.5).*

Otra forma, de evaluar el cumplimiento legal, es atender a la Ley Federal de Derechos de Autor, que en su artículo 6° respalda la fijación de elementos de creación personal en los contenidos, el artículo 102 que protege el código del programa como una obra literaria, el artículo 103 que observa los derechos patrimoniales de una obra colectiva y el artículo 113 que brinda protección a la transmisión de la obra por redes de telecomunicaciones. De manera alterna, resulta de interés la Ley de la Propiedad Industrial, que en su artículo 2° se encarga de la regulación y otorgamiento de patentes de invención.

Figura 5. Logotipos del OMPI e IMPI

Fuente: [Elaboración propia con logotipos citados en, IMPI y OMPI]

c) *Confiabilidad de las transacciones electrónicas*

El uso de *internet* como medio para comprar y vender productos y servicios no está exento de acciones fraudulentas; la aplicación del artículo 46 y 76 Bis de la Ley Federal de Protección al Consumidor, indican como obligación del sitio *web* presentar información adicional en las promociones y ofertas de los productos; así también estipula los derechos de los consumidores en las transacciones electrónicas, garantizando la confidencialidad de los datos, la aceptación de la calidad y cantidad de productos solicitados, la difusión de formas y condiciones de pago, y en especial los términos de cargos adicionales.

Otro aspecto tipificado en el artículo 6 bis del Código de Comercio, es la presencia de material que induzca a una competencia deshonesta con otros comerciantes; la actualización constante del listado de precios juega un papel muy delicado al momento realizar los pedidos electrónicos, unos segundos son la diferencia entre el precio viejo y el nuevo, pero el dueño está

obligado por el artículo 1860 del Código Civil Federal, a sostener el precio de la mercancía con el cual fue ofertado al público al momento de realizar la transacción.

Para asegurar que el sitio cumple con todos los requerimientos de ley es necesario identificar el nombre legal de la empresa, dirección fiscal, teléfono y fax de contacto; cada producto debe de presentar en forma visible, su precio en moneda nacional, cargo adicional por el servicio de envío, las condiciones y formas de pago, tiempos de entrega según el área geográfica, restricciones en cantidades solicitadas, asimismo señalar las especificaciones cuando se presente una devolución o el reenvío de la mercancía o del efectivo.

Finalmente, el manejo de los datos de carácter personal como los nombres, correo electrónico y números de tarjetas de crédito de los clientes deberán ser protegidos por políticas de privacidad claramente expuestas, entre las más señaladas figuran que los datos solicitados solo se emplearan para realizar contacto en relación a su pedido y que estarán protegidos de ser reproducidos, compartidos o comercializados.

El uso de *internet* no tiene un cuerpo jurídico en la legislación mexicana, cualquier persona con un equipo de cómputo fijo o móvil, puede acceder a miles de páginas sin restricción alguna, sin embargo como usuario del servicio debe comprobarse que se tiene una concesión para instalar, operar o explotar redes públicas, tal como lo dispone el artículo 24 de la Ley Federal de Telecomunicaciones.

d) Confidencialidad de datos personales

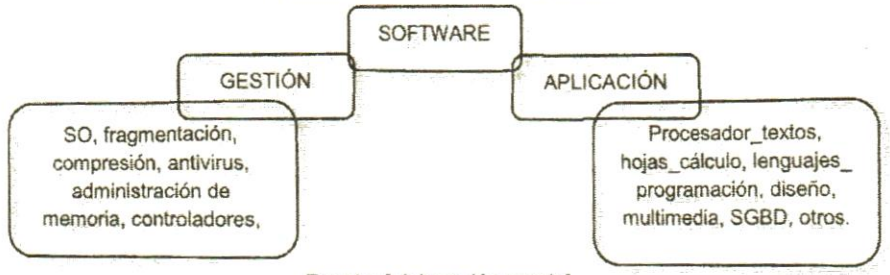
Cuando se emplean formularios para registrar los datos de los clientes y proveedores, inmediatamente hay que asegurar la protección de los mismos, entre los aspectos que debe considerar el portal *web* es la denominación social, el domicilio fiscal, el consentimiento del cliente en base al motivo por el cual se solicitan los datos, el aviso de privacidad y la garantía de uso, asimismo la opción para modificar o cancelar la información por parte de los usuarios en cualquier momento. El incumplimiento de estas acciones viola los derechos regulados por la Ley Federal de Protección de Datos.

1.3.2. Auditoría de *Software*

Los sistemas informáticos se componen principalmente de *hardware* y *software;* el primero corresponde a las partes físicas o tangibles y el segundo a las partes lógicas o intangibles, éstos se han ido implementando en el desarrollo de los procesos institucionales, llegando a ser una parte medular de las mismas actividades, en donde la complejidad de los mismos han ido evolucionado acorde a los avances tecnológicos, ofreciendo nuevos retos a los administradores y auditores

Cuando se habla de *software* se alude a gran variedad de programas, tales como sistemas operativos, sistemas administradores de base de datos, procesadores de textos, hojas de cálculo, antivirus, controladores, lenguajes de programación y otros. Como se puede apreciar en la imagen siguiente *(ver Fig.6).*

Figura 6. Clasificación de Software



Fuente: [elaboración propia]

Entre los aspectos que se deben supervisar en cada uno de ellos son:

1.3.2.1. Adquisición

Es un proceso que involucra a los proveedores y entre las principales interrogantes que se deben responder, se encuentran las siguientes: ¿por qué se eligió el *software* actual?, ¿quién es el responsable de adquirir el recurso? y ¿qué servicios ofrecen los proveedores?, las repuestas a éstas preguntas, ofrecen información adicional para saber si existe un mecanismo formal que incluya la solicitud y aprobación del recurso; si la petición está en función de la dependencia con otros programas; si incluye los servicios de asesoría en línea o personal, adiestramiento, actualizaciones en línea y automáticas, y finalmente el tiempo de garantía que pueda ofrecer un proveedor, y el reconocimiento nacional o internacional del mismo.

1.3.2.2. Administración

Es un rubro que se interesa por el rendimiento y ejecución de sus programas es por eso que lleva el control del número y tipo de *software* instalado, el espacio ocupado y disponible de memoria RAM conocida de esta manera por sus siglas en inglés *Random Access Memory*, asimismo, el número y capacidad de discos duros, su espacio ocupado y disponible, el conocimiento del sistema de archivo, controladores o *drivers* y las especificaciones del microprocesador de cada equipo, operación que se deberá repetir el número de veces que corresponda al número de máquinas existentes. Así también deben revisarse estadísticas de uso y documentación de *software*, que incluye contratos con proveedores, manual de usuario, códigos y diagramas.

1.3.2.3. Licenciamiento

Se enfoca estrictamente en conocer el estado de instalación de cada recurso, en los programas "propietarios", se debe verificar que el usuario cuente con la licencia correspondiente y comprobar que los derechos otorgados no sean extralimitados en relación a la reproducción de los mismos; pero en los programas de "distribución libre", se debe considerar el derecho de ser usados, modificados y distribuidos bajo los términos de las licencias GLP, AGLP, BSD y MPL, de las cuales se pueden derivar los programas con licencia *CopyLeft* que son empleados por desarrolladores para realizar aplicaciones para las áreas de negocio y registrar sus derechos con licencia *CopyRight*, la única obligación de esta modalidad es otorgar de manera proporcional los ingresos correspondientes a los autores por la transmisión de los derechos patrimoniales, según el artículo 31 de la Ley Federal de Derechos de Autor, sin excepción alguna, ya que existen empresas que evaden esta responsabilidad declarando que la obra también será a título gratuito o por contrato oneroso sin especificación de características violando sistemáticamente la legislación nacional.

Por último, existe otro grupo de programas, de descarga gratuita que permiten su instalación por poco días y con funciones limitadas, brindando la opción de pagar un importe estipulado si se desea obtener la versión completa.

1.3.2.4. Seguridad

Es un tema delicado, cuando las empresas conocen los riesgos y miden sus consecuencias, la probabilidad de que ocurran depende directamente de la naturaleza de las operaciones, es por eso que los altos directivos invierten en candados para proteger los datos como el activo más preciado ante la intromisión de usuarios no autorizados o la filtración de virus al sistema, que ocasionen daños temporales o permanentes a la integridad de los archivos.

Un administrador de tecnologías está consciente que lo que *"el hombre hace, él lo deshace"*, con la frase anterior se trata de explicar que la misma capacidad humana que se emplea para crear líneas de código para autentificar y autorizar el acceso a los usuarios; es empleada para violar el algoritmo de seguridad, por lo tanto, hablando técnicamente, se podría decir "que no existe un sistema seguro, a menos que éste se encuentre apagado".

Ante la necesidad imperante de emplear sistemas informáticos en las áreas de negocios, es obligación del auditor evaluar las medidas de seguridad de las transacciones digitales, tales como:

a) Contraseñas

Son consideradas las puertas de acceso al sistema, que deben cumplir con una actualización periódica y permanente, que además se deben formar de letras, números y símbolos, que incluyan como mínimo 8 caracteres, y que empleen de preferencia el código CAPTCHA, así también se consideran algunos métodos biométricos como la palma de la mano y la huella dactilar que por su precio y accesibilidad son más comunes.

La seguridad no se limita solo en el acceso, sino también se puede configurar por medio de niveles *(ver Fig.7)*, por ejemplo:

Nivel 1. **BIOS**: Cuando se habilita esta contraseña, el ordenador no puede cargar la rutina de arranque de la ROM BIOS, conocido por sus siglas en inglés *Read Only Memory* y *Basic Input/Output System.*

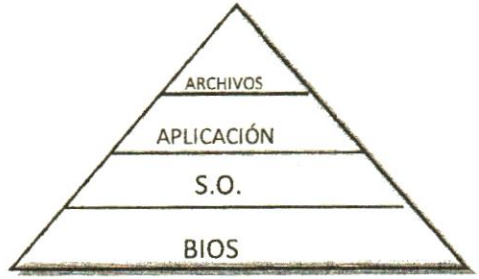
Nivel 2. **Sistema Operativo**: Al encender la computadora, inicia el proceso de testeo de *hardware*, pero no permite inicializar *Windows, Linux, Mac, Solaris* u otro sistema operativo que se encuentre instalado, hasta no teclear la clave correcta.

Nivel 3. **Aplicaciones:** Después de encender el ordenador e inicializar el sistema operativo, debe seleccionarse el *software* de aplicación que se empleará para la administración de los datos, la mayoría de los fabricantes solicitan el nombre y la contraseña del usuario, como medidas de

seguridad. También existen los sistemas de información; éstos son programados por expertos, que además del candado de inicio de sesión, incluyen protección de transacciones a través de la asignación de privilegios y roles por usuarios.

Nivel 4. **Archivos:** Al ingresar a una aplicación y abrir una sesión de trabajo, se genera un documento, que aplica las protecciones de lectura y/o escritura si posteriormente se desea actualizar o eliminar.

Figura 7. Niveles de Seguridad con Software

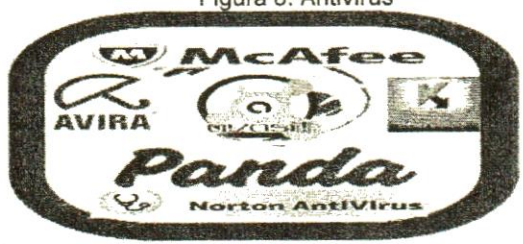


Fuente: [elaboración propia]

b) ***Antivirus***

En el listado de *software* del ordenador, sin excusa alguna debe figurar el nombre de un programa residente en memoria que brinde la protección al equipo contra el *malware* y *spyware*. El nivel de protección, está relacionado a los siguientes requisitos: asistencia técnica, actualización constante, detección de nuevos virus, respaldos de emergencia y tipo de adquisición. Entre los más citados por su capacidad de detección podemos citar: *Karpersky, Avast, Avira, AVG McAfee, Norton Antivirus y Panda Cloud,* entre otros, *(ver Fig.8).*

Figura 8. Antivirus



Fuente: [elaboración propia con Logotipos existentes en internet]

c) ***Cifrado***

Es una medida de protección, que debe de estar contemplada en la información sensible de la empresa, para reducir el riesgo de ser sustraída indebidamente, las formas en que se pueden presentar es por medio de la configuración avanzada de seguridad que tiene cada *software* de aplicación, o empleando programas específicos que automaticen la tarea de encriptación y desencriptación, tales como: *Cryptainer, Cryptoforge, AxCrypt y Criptod* y, para los casos especiales a través de la codificación programada por expertos.

d) ***Bloqueo de puertos***

Los puertos *Universal Serial Bus* reconocidos por sus siglas en inglés como USB y las unidades lectoras de memorias *Flash*, son una forma de prevenir el robo de información, para supervisar el control de acceso de los dispositivos de almacenamiento, se pueden presentar diferentes casos, en donde el más vulnerable sería cuando el responsable del equipo autoriza el ingreso de los dispositivos al ordenador, debido a que existirá el riesgo de un acceso no autorizado; pero existen otras formas que pueden combinarse con la anterior o emplearse por sí solas para monitorear y controlar los puertos.

Una de ellas sería comprobar la existencia de un antivirus que contenga activa la opción de "configurar el acceso de los puertos", un ejemplo podría ser el NOD 32; también existen aplicaciones de *software* con la misma finalidad, entre la cuales destacan: *MyUSBOnly, USBsafeguard y USBLocker*, entre otras; en esta sección, también se hace mención de *Rohos Logon Key*, que incluye una característica diferente, la cual consiste en emplear la memoria como una llave personal para acceder al equipo.

Pero, todas estas medidas de seguridad quedan inservibles al momento de permitir el acceso y no revisar el contenido de los dispositivos de almacenamiento, en los cuales se pueden alojar archivos ejecutables en carpetas ocultas con la única función de hurtar las contraseñas y los seriales de cada programa de manera sigilosa, asimismo, quedan vulnerables los datos confidenciales que se describirán posteriormente en seguridad de redes.

Para compensar esta debilidad, es necesario registrar los accesos a los puertos, que indique el usuario que realiza la acción, la descripción del movimiento, la fecha y hora. Hoy en día existen herramientas de apoyo que ofrecen al auditor un reporte individual y especifico de los programas, entre

las cuales puede mencionsarse a: *Winaudit, OpenAudit, FreshDiagnose, Softkey y Everest.*

1.3.3. Auditoría de Base de Datos

La Base de Datos se ha convertido en la columna vertebral de los sistemas de información, al reconocer los directivos la importancia que tiene el administrar correctamente la información en un mundo de negocios donde la Atomicidad, Consistencia, Aislamiento y Durabilidad -propiedades ACID- de las transacciones en un Sistema de Gestión de Base de Datos "SGBD" marcan el éxito de las empresas. Una buena auditoría no solamente se basa en la revisión del diseño lógico e implementación física de la base de datos para detectar los riesgos en las operaciones de creación, eliminación, modificación y consultas, que se pueden estar presentando y no ser detectados en el trabajo cotidiano; sino también en observar la forma en que interactúan con otros usuarios y sistemas para descartar vulnerabilidades en su uso. Es por ello que, para evaluar el funcionamiento adecuado, es necesario analizar los controles que se emplean en el área técnica y administrativa.

1.3.3.1. Técnica

Se requieren conocimientos especializados en sistemas que permitan evaluar un control de acceso legítimo a través de la existencia de cuentas y contraseñas, en donde éstas últimas deberán formarse por la combinación de letras, caracteres, espacios y/o números; un usuario autorizado debe pertenecer a una clasificación y tener asignados privilegios, mismos que pueden ser revocados o propagados; para el control de privilegios, es necesario verificar la existencia de un historial que contenga al usuario emisor, usuario receptor, operaciones y tiempo autorizado; para el control de transacciones, una bitácora es necesaria para almacenar un *log* o registro de todas las operaciones que realizan los usuarios durante una sesión con puntos de confirmación y de control que protejan a las operaciones confirmadas de una reversión en cascada en el caso de una caída del sistema; para el control de recuperación asegurar que se emplean técnicas para la restauración de la base de datos; para el control de acceso remoto se debe monitorear e identificar las direcciones IP de las terminales, el tipo de paquetes que se enviaron, y el tipo de acceso autorizado o no autorizado,

cuando ocurre el segundo caso, se deben tener Sistemas de Detección de Intrusos denominado por sus siglas en inglés IDS, que se activen en tiempo real para notificar al administrador el acceso ilegal de usuarios o la ejecución de actividades maliciosas. La implementación del IDS basados en conocimiento, comportamiento, redes y/o *host* basados en conocimiento, comportamiento, redes y/o *host* se define en el modelo de seguridad, para evaluar su control deben cumplir los siguientes requisitos: ser autómata, tolerante a la caída del sistema, auto-evaluable y adaptable a los sistemas y aplicaciones. Las herramientas de apoyo en esta área son *Secure Oracle Auditor, Secure SQL Auditor*.

1.3.3.2. Administrativa

La evaluación de los procesos debe iniciar con la revisión de los lineamientos establecidos en las políticas internas para supervisar que sean contemplados y después continuar evaluando el grado de cumplimiento. A continuación se mencionan algunos procesos que deben tener una normativa definida:

a) *El acceso de los usuarios,* debe considerar actualizaciones periódicas de las contraseñas, con los requisitos de mayúsculas, minúsculas, números y espacios, generados automáticamente por el sistema y un protocolo de entrega al usuario correspondiente por parte del administrador.

b) *La confidencialidad de los ficheros*, exige que el responsable de la base de datos esté sujeto a disposiciones contractuales para el aseguramiento de la información, y en caso de incumplimiento podría ser sancionado con una pena de 10 años de cárcel, según artículo 69 de la Ley Federal de protección de Datos; también brinda al usuario titular el derecho de acceder, actualizar, eliminar y excluir información de cualquier tratamiento, según artículo 63 y obliga a las empresas a cumplir con el aviso de privacidad apegado a las normas del Instituto Federal de Acceso a la Información y Protección de Datos, conocido por su siglas como IFAI. Los niveles de seguridad se clasifican de la siguiente manera: el primer nivel se denomina básico y resguarda el nombre, domicilio, teléfono, edad, sexo, fecha de nacimiento y nacionalidad; el segundo nivel se le conoce como medio y asegura la información financiera, legal y psicológica, y por último se encuentra el tercero, llamado alto que se encarga de vigilar información relacionada al origen racial, preferencia sexual, religiosa y política del usuario.

c) En el ***respaldo de información,*** se deben definir los datos personales del encargado responsable, los datos a respaldar, los periodos de ejecución -semanas, días o turnos- y los medios de almacenamientos; éstos últimos pueden ser: fijos, extraíbles o a través de la *web*, y cuando se realiza por discos duros o cintas magnéticas se recomienda que se guarden afuera de las instalaciones. Entre las técnicas más usuales esta RAID que ordena discos duros y almacena los mismos datos en cada uno de ellos, es útil para los protocolos de recuperación, porque el cambio de un disco dañado se realiza en caliente mientras que otro se encuentra en proceso de grabación.

d) En ***eliminación de ficheros***, se otorga como derecho al titular de los datos en el momento que él desee y como obligación de ejecutar la petición al responsable de la base en datos, según artículo 11 de la Ley Federal de Protección de Datos.

1.3.4. Auditoría de Redes

Las redes de área amplia y local denominadas WAN y LAN por sus siglas en inglés *Wide Area Network* y *Local Area Network* respectivamente, son el punto más vulnerable de la organización, por ser el principal medio de intercambio de información a través de correos electrónicos, mensajería instantánea, formularios de datos en sitios *web*, redes sociales, y más. De esta misma manera, el b*luetooh* y el infrarrojo como medios de comunicación inalámbrica de corta distancia también son susceptibles a los ataques.

1.3.4.1. Seguridad Lógica

"La mejor forma de comprobar el nivel de seguridad contra intrusos es auto-atacar", evitar los ataques de intrusos es proteger el sistema de actividades fraudulentas, que no pueden ser detectadas por medios físico sino a través del mismo sistema. Entre los aspectos más relevantes a supervisar el modo de operación, se encuentran:

***a) Contraseñas de acceso WiFi*:** Los métodos de autentificación más comunes para los dispositivos que emplea cualquier tecnología inalámbrica *WiFi* por sus siglas en inglés *Wireless Fidelity*, son *Wi-Fi Protected Access* reconocidas por su acrónimo WPA y WPA2, siendo el último el más confiable y adaptable, porque cuenta con la versión personal para redes domésticas con una clave a varios usuarios y la empresarial para servidores 802.1X, con claves diferentes por cada usuario. Un método más antiguo y no recomendable por la facilidad de acceso de intrusos, es el *Wired Equivalent*

Privacy denominado por sus siglas en inglés como WEP; es un sistema abierto y con clave compartida. (Microsoft, Windows, 2013).

La importancia de administrar correctamente el nombre y la clave de la red, se debe a que actualmente existen muchas aplicaciones que en minutos descifran contraseñas, entre algunas pueden mencionarse: *Beini, AirCrack, Backtrack, Wifi Way y Wifi Auditor* todas son aplicables a cifrados WEP/WAP de cuatro o seis dígitos y su uso depende exclusivamente del interés de la persona; por ejemplo, un administrador puede emplearla para recuperar una contraseña y un auditor para evaluar el nivel de seguridad, pero, también existen *hackers* con el objetivo expreso de ingresar ilegalmente.

b) Registro de actividades por usuarios*:* la mejor forma de asegurar el uso de la red, es conocer la IP de las computadoras que se conectan a *internet;* el rastreo se puede realizar con los siguientes programas *AY Spy, Visual Zone Report Utility y IP Lookup,* entre otros, hoy en día también existen páginas que facilitan el rastreo como *WhatIsMyIPAddress.com* con solo ingresar la dirección buscada, aunque son buenas prácticas de seguridad y brindan la información geográfica (país, estado, latitud y altitud), no hay que ignorar los programas simuladores de IP que cambian el origen real de la conexión, tales como: *IP Swapper y Hide IP Easy.*

***c) Comunicación segura*:** es un reto a través de *internet,* y una forma de resistir a los ataques del robo de paquetes es usando el protocolo HTTPS -HyperText Transfer Protocol with Privacy- con el puerto 443 y el método de encriptación SSL/TLS -*Secure Sockets Layer /Transport Layer Security*-; éstos sitios se distinguen de otros por el uso de los certificados digitales, los cuales son avalados por una Autoridad Certificadora (AC) que garantiza la posesión de los datos por la entidad autorizada. El documento contiene el nombre, dirección, correo electrónico, organización y llave pública del propietario, además de información pertinente del certificado, como periodo de validez, número de serie, AC, firma digital de la AC cifrada con su llave privada. Una forma de identificar los sitios seguros es observar en el navegador *web* un "candado" a lado de la URL, entre algunos ejemplos sobresalen: *Facebook, Twitter, Google, Hotmail, Yahoo, Youtube,* Telcel y Telmex.

Aunque este protocolo tenga menos riesgos, siempre está latente la posibilidad de ser atacado por usuarios con la suficiente habilidad para interceptar y descifrar paquetes por medio de un certificado falso, (Ramírez & Espinoza, 2011).

Las recomendaciones a seguir para aumentar el nivel de seguridad de la red serían: ocultar el identificador de red SSID, usar de preferencia el cifrado WAP2, cambiar la contraseña que trae por defecto, colocar contraseñas con palabras mayúsculas, minúsculas, números y caracteres, configurar el *router* para que no acepte dispositivos en forma automática, actualizar antivirus y navegadores, evitar redes públicas en transacciones electrónicas y confirmar la existencia de certificados en protocolos HTTPS, traducido por su siglas en español a Protocolo Seguro de Transferencia de Hipertexto.

d) La Compresión y descompresión de archivos por correo electrónico es de gran utilidad para reducir el tiempo de transferencia y aumentar la capacidad de almacenamiento de los dispositivos. Cuando se requiere comprimir uno o más archivos se deben emplear programas como *Winrar y Winzip,* ambos soportan formatos zip, rar, cab, tar, iso, img, entre otros.

e) La exportación e importación de base de datos en ambiente Web se presenta ante la necesidad de realizar alojamientos o copias de seguridad, la forma común de realizar la migración es a través de la línea de comando o *Shell,* en el caso especial de *MySql* se puede emplear la herramienta *phpMyAdmin.*

f) Tasas de errores de transmisión, en un canal de comunicación que transporta datos, siempre ésta latente la posibilidad de que el enlace sea corrompido, por lo general mientras mayor sea el tamaño de la trama, mayor es el riesgo.

Cuando los errores son visibles lo importante es detectarlos anticipadamente, entre los mecanismos a emplear se encuentran los de verificación de redundancia vertical, horizontal y cíclica en el envío de los datos conocidos como VRC, LRC y CRC; esto ocasiona disminución en la velocidad de transmisión, pero a cambio asegura su integridad; otra forma de detección, son las técnicas ARQ o de parada-espera que se encarga de controlar el flujo de tramas entre el ordenador y el *modem.*

Además, existen herramientas que permiten mejorar la seguridad de las redes haciendo un análisis de los paquetes de red que se transmiten en una conexión, entre los que figuran: *Wireshark, OptiView Networks Analizer, Total Network Inventory y Tcpdump (*modo consola*).*

g) Protección de puertos, se trata de colocar candados por medio de programas como:*MyUSBOnly, USBsafeguard o USBLocker* que impidan las

filtración de archivos ejecutables denominados "*Roba-datos*" diseñados para copiar información confidencial de una computadora, en especial las contraseñas y el historial de navegación, a través de los puertos USB, memorias *flash* y otros dispositivos.

1.3.4.2. Seguridad Física

a) ***Área de los servidores***. Una instalación protegida se relaciona con los mecanismos de seguridad implementados, entre ellos se mencionan las puertas con cerraduras, alarmas contra intrusos, métodos de accesos biométricos, digitales o manuales; vigilancia personal o con cámaras de video, registro de usuarios, bitácora de actividades, control de temperatura ambiente, de ventilación y de iluminación; área aislada de interferencia electromagnética, uso de material de construcción antiestático e inflamable, incluyendo la pintura y el material del mobiliario; la ubicación geográfica dentro de la organización debe ser alejada del flujo continuo de las personas, de tuberías y cauce de vertientes acuíferas; el sistema de alarma debe contar con mecanismos de detección de sismos y de incendios; asimismo, detector de medios electrónicos de almacenamiento, como: USB, discos compactos, memorias, etc.; el laboratorio debe incluir puertas de emergencia y extintores según los metros cuadrados del área y el aforo de la misma; contar con la instalación a tierra y de para rayos, si se encuentra en una zona de lluvias eléctricas; la instalación eléctrica debe ser de preferencia con cable 10, conectores trifásicos y cable oculto, reguladores o *ups*; la instalación de los cables de red debe incluir código por línea, estar separada de los cables telefónicos y estar ocultos a la vista del usuario; se deben evitar puertas o ventanales de cristales; sancionar por introducir comida, bebidas, cigarros y sustancias prohibidas, y contar con procedimientos para la destrucción de papelería o archivos digitales.

b) ***Equipos para el tráfico de red.*** Para garantizar la eficacia de una conectividad de alto rendimiento y confiabilidad es importante contar con el manual de instalación, operación y mantenimiento de *routers* y *switches*, entre las características aprobatorias "se encuentran los equipos Cisco con 48 puertos RJ-45, velocidad de transmisión 1000Mbps, medio de transmisión *Store and forwa*rd, protocolos de ruteo RIP, topología estrella y disponibilidad para la escalabilidad del equipo" (Rodriguez 2005).

Los *Firewall* se pueden encontrar en los *router* o en el sistema operativo, ambos tienen la misma función de proteger los recursos que se comparten en la red, para aprobar una auditoría se debe demostrar la capacidad de detectar y bloquear a usuarios no autorizados que intenten

ingresar y asimismo fortalecer los puertos que han sido perpetrados, uno de los *router* más recomendables es ASA 5500 de Cisco con VPN/IP –para seguridad IP- o VPN/SSL -con *sockets* seguros-. Las herramientas de apoyo sugeridas son: *CIS Router Audit Tool* que se especializa en equipo Cisco y Nipper, programa de código abierto adaptable a cualquier plataforma de sistema operativo.

c) ***Respaldos.*** Inician con una política y un protocolo de recuperación, los medios pueden ser en otro servidor, cintas, discos duros o alojamiento web, que deben estar ubicados en lugares externos y seguros, también existen instituciones reconocidas a nivel internacional y nacional para la custodia y protección de la información, un ejemplo podría ser: *IronMountain.*

d) ***Usuarios***. Emplear estrategias para regular la conducta de las personas, fortalece la seguridad, diseñar y difundir reglamentos que especifique la prohibición de introducir memorias extraíbles, descargas de programas, reenvío de cadenas de correos y no abrir correos electrónicos con destinario desconocido.

1.3.5. Auditoría de *Hardware*

Cuando se alude al *hardware* se refiere a las partes tangibles del equipo incluyendo sus periféricos, éstos activos representan una inversión importante para la empresa y como tal, se debe tener el conocimiento exacto del recurso con el que se cuenta.

1.3.5.1. Adquisición

Cuando se decide comprar un equipo, se justifica a través de una solicitud realizada por el experto en el área, que contenga las características específicas del recurso y que sea aprobada por la Dirección. El procedimiento también incluye la elección del proveedor, dependiendo de las garantías que ofrezca en relación al costo, tiempo de entrega, servicio de mantenimiento, seguro del equipo, asistencia en línea y alternativas de escalabilidad, en relación a la capacidad de memoria RAM y Disco duro principalmente,

1.3.5.2. Inventario

El control del recurso tecnológico, consiste en asignar un número de identificación a los equipos portátiles, que pueden ser representados por *laptos*, *netbook* y *tablet´s*, también a las computadoras de escritorio

incluyendo monitor, teclado y ratón, y de la misma manera a impresoras, *scanner, switches*, servidores, reguladores y supresores, que todos juntos colaboran en la función informática, si se requiere de un registro más detallado se incluyen las propiedades del microprocesador, memoria RAM, disco duro, tarjetas de video, sonido y red; registro que debe actualizarse constantemente, afortunadamente para disminuir el esfuerzo de esta ardua labor existe *software* específico que extrae automáticamente los datos de cada computadora: *Winaudit, OpenAudit, FreshDiagnose, Softkey y Everest.* Otro registro importante en el uso del equipo, que se puede representar a través de estadísticas o gráficas para visualizar mejor la relación entre usuario-equipo o equipo-horas.

1.3.5.3. Seguridad

Las medidas preventivas para evitar el robo de un computador pueden ser: cámaras de seguridad, vigilancia personal o programas automatizados, que se activan cuando se denuncia el delito, capturando la imagen y ubicación geográfica más próxima del delincuente cuando se conecte a *internet* con el equipo robado y envía por correo electrónico la información al usuario afectado; unas de las herramientas más reconocidas para esta actividad, son: *Snuko y Prey.*

1.3.5.4. Instalaciones

La infraestructura y mobiliario son elementos que determinan la conservación del *hardware* y la seguridad de los usuarios, entre las características a observar se debe verificar la existencia, difusión y aplicación de un reglamento interno del uso de las instalaciones, del análisis de riesgos, y de los planes de contingencia y/o de continuidad.

Un edificio de cómputo debe cumplir medidas de seguridad, en relación a:

a) La **ubicación geográfica** dentro de la organización determina el grado de exposición del mismo al personal externo y reduce el nivel de riesgos a robo, sabotaje y vandalismo.

b) Los **accesos disponibles** deben estar en función al número de usuario y al área del edificio, debe considerarse la forma y medida correcta de las puertas de entrada, de salida y de emergencia.

c) La **ventilación e iluminación del inmueble** debe incluir además del clima acondicionado, ventanas de tamaño adecuado que se puedan abrir

para evitar la humedad, que regulen la incidencia de los rayos del sol y que no deje al descubierto el área de trabajo a las personas ajenas; asimismo, se debe considerar el número y tipo de lámparas de uso normal y de emergencia.

d) Las **instalaciones eléctricas** en México deben basarse en la norma NOM-001-SEDE-2012 que se enfoca a equipos de uso general y sistemas de comunicación, otra forma de asegurar el equipo es la ubicación estratégica de conectores, instalaciones a tierra, reguladores, UPS (fuente de poder interrumpible) y ahorradores de energía.

e) **Mobiliario**; las sillas, mesas y estantes, deben de estar distribuidos correctamente para brindar comodidad al usuarios y adaptados eficientemente al equipo para su buen funcionamiento.

f) La **prevención de un incendio** debe incluirse en el plan de emergencia, asimismo, ser considerado en la asignación de funciones y simulacros efectuados por el personal que labora en el área; las instalaciones deben estar equipada con alarmas contra incendio, rutas de evacuación y extintores PSQ (Polvo Químico Seco) clase C para equipos eléctricos energizados y/o Halogenados (Hexafluoro Propano/Halotrón) para computadoras. Las paredes, pisos y techos, así como la pintura de los mismos, son determinantes para la conducción del fuego, por lo tanto, es importante observar el material de construcción.

g) La **prevención de desastres naturales**, tales como sismos, inundaciones, tormentas eléctricas, huracanes y otros, deberán contar con planes bien definidos e infraestructura adecuada.

1.3.5.5. Destrucción

Cuando la vida útil del equipo ha llegado a su fin surge la interrogante de ¿qué hacer con ese equipo? y cuando se trata del disco duro en especial, no basta con eliminar los datos para que éstos dejen de existir; es por ello, que en muchas ocasiones se recurre al formateo, al campo magnetizado, a una hoguera o simplemente a martillazos, aunque son opciones extremista siempre existirá el riesgo que la destrucción sea incompleta; muchos administradores preocupados por la confidencialidad de los datos han optado por adquirir unidades de trituración que se encargan de perforar los platos, asegurando la destrucción total de la información en segundos, un ejemplo podría ser el *Hard Disk Destruction de EDR solutions,* o contratar los servicios

de empresas profesionales como *Intermex S.L.*, que validan el proceso con un certificado de destrucción o por *Shred-It* que ofrece servicio móvil de destrucción de información en las mismas instalaciones. Estas medidas son necesarias ante la habilidad que ha adquirido el ser humano para la recuperación de datos y restauración de discos duros; como sería el caso del *Grupo IDEA Informática*, Desarrollo, Equipo y Asesorías S. de R.L. de C.V., formado por profesionales, con el objetivo de aplicar informática forense dentro de un marco legal.

1.3.5.6. Reciclaje

Es un tema de interés internacional para la prevención de contaminación al medio ambiente, es por eso, que una actitud responsable sería contar con un sistema de gestión ambiental, preferentemente normada por *International Standard Organization* (ISO 14000); o en su defecto por políticas, metas y estrategias institucionales para el desarrollo sustentable. Existen empresas en espera de la donación de los recursos, entre algunas puede mencionarse: *Summit´s Electronic Recycling, Eco-Azteca Recicladora,* y *Centro de Recolección y Reciclaje de Computadoras (CRRC),* ésta última creada por estudiantes de la Universidad Autónoma de la Ciudad de México (UACM). Las computadoras portátiles y de escritorio, tabletas, servidores, *router, switches* y reguladores, cargadores, celulares, reproductores de DVD y otros; se convierten en basura electrónica tóxica cuando empiezan a liberar metales peligrosos como el berilio, cromo, cobre, arsénico, selenio, mercurio, cadmio y el plomo, ocasionando daños irreversibles a la salud. Es por ello que los programas de Reparación, Reciclaje y Reducción (RRR) son una excelente opción para los equipos que han sido declarados descontinuados o defectuosos.

CAPÍTULO II

NORMAS LEGALES

Código Penal Federal
Ley Federal de Telecomunicaciones
Ley Federal de Derechos de Autor
Ley de la Propiedad Industrial
Ley Federal de Protección al Consumidor
Ley de Protección de Datos Personales en Posesión de Particulares
Ley SOX (*Sarbanes-Oaxley*)
Ley SOPA (*Stop Online Piracy Act*)

2.1. La Legislación Mexicana en la Auditoría Informática

En México la frase "*lo que no está prohibido, está permitido*", parecería una forma de reflejar la situación de la auditoría en informática prevaleciente.

A través de los años se han creado y fortalecido las normas legales para proteger la seguridad de la información, pero aún quedan espacios por llenar. Para comprender mejor esta situación se apuntan las siguientes observaciones:

- Primero: la naturaleza evolutiva de la tecnología en el contexto informático promueve la creación de nuevos delitos que no se encuentran específicamente tipificados en los códigos de conducta, por ello al momento de dictaminar la sanción y/o multa correspondiente, los encargados de impartir justicia se ven en la necesidad de escoger el delito que más se asemeje.

- Segundo: las leyes mexicanas han proliferado en forma desmedida para indicar los derechos y obligaciones de las personas en relación a los servicios y productos; que en ocasiones, puede observarse que un artículo es considerado en dos o más legislaturas; cuando ocurre esto, puede ser muy útil para reforzar los argumentos de una sentencia; así también, puede ser perjudicial, ante la posibilidad de causar una confusión por el enfoque de aplicación y en el caso más delicado, puede originar una contradicción cuando una obligación se contrapone con otra, provocando la anulación o reducción de la sanción.

- Tercero: la relación compleja que guardan las empresas mexicanas con normas extranjeras o estándares internacionales, cuando se trata de regular procedimientos y procesos internos que se emplean en la adquisición y venta de productos y/o servicios de comunicación, así como la transmisión, almacenamiento y/o procesamiento de información.

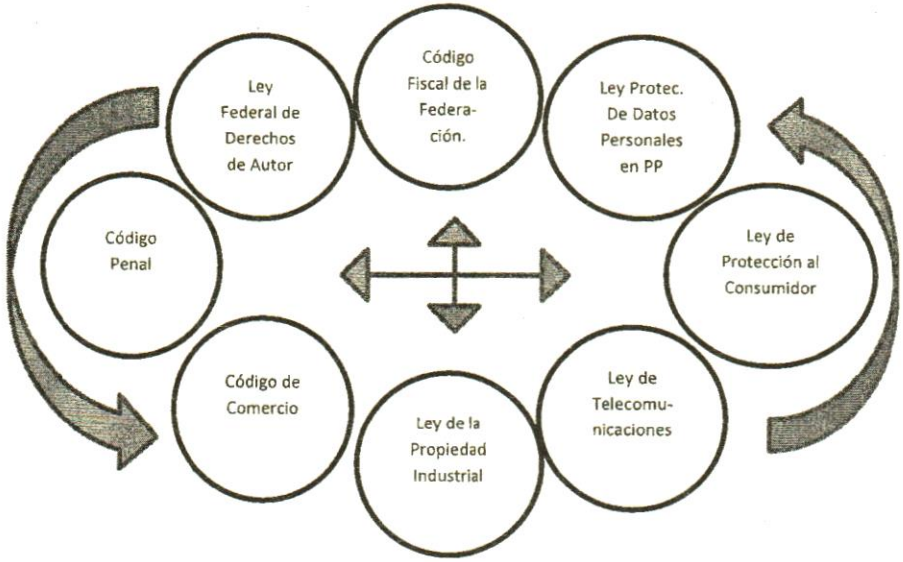
2.2. Normas mexicanas

Cuando se aluden a las normas nacionales, inmediatamente viene a la memoria una gran cantidad de códigos y leyes con capítulos y artículos que regulan la conducta humana; que en muchas ocasiones, por la ignorancia en la materia no son interpretadas adecuadamente, o en otros casos, por desconocimiento de su existencia se actúa fuera del marco legal.

En un proceso de auditoría en informática, es necesario tener conocimientos legales para indicar qué faltas se están cometiendo y el grado de gravedad de las mismas.

Es por eso, que en este capítulo se presentarán de la manera más breve posible, una serie de disposiciones legales (*ver Fig.9*) con los artículos más sobresalientes en el área de estudio para conocer su contenido y sanción correspondiente; acompañados de un caso práctico que permita analizar una situación real.

Figura 9. Normas mexicanas



Fuente: [elaboración propia]

2.2.1. Código Penal Federal

Basados en el contenido de este ordenamiento cuyo objetivo es regular la conducta humana en relación a las actividades delictivas relacionadas con el uso indebido de los sistemas de información, equipos de tecnológicos y de comunicación, destacan:

Artículo 168 bis. Sanción de 6 meses a 2 años de prisión, a quien sin derecho decodifique o permita descifrar señales de telecomunicaciones.

Artículo 173. Sanción de 180 jornadas de trabajo en favor de la comunidad, a quien abra un escrito que no esté dirigido a él.

Artículo 177. Sanción de 12 años de prisión, a quien intervenga comunicaciones privadas.

Artículo 178 Bis. Sanción de 2,500 días multa, al operativo de la concesionaria que se rehúse a colaborar con las autoridades en investigaciones del servicio de telecomunicaciones.

Artículo 210. Sanción de 200 jornadas de trabajo en favor de la comunidad, a quien sin derecho revele información obtenida por su cargo.

Artículo 211. Sanción de 5 años y suspensión de un año de su profesión, a quien sin derecho revele información o imágenes de carácter industrial obtenidas por su cargo o en una intervención de comunicación privada.

Artículo 211 bis 1-6. Sanción de 4 a 12 años de prisión, a quien sin derecho destruya, altere o copie información con un nivel de seguridad, contenida en equipos o medios de almacenamientos informáticos de particulares, empresariales, del Estado y del sistema financiero. Además, la destitución del cargo, si el responsable es un servidor público.

Artículo 220. Sanciona el ejercicio abusivo de funciones, cuando el servidor público produzca un beneficio económico con la información que posee por su cargo.

Artículo 368. Sanciona como robo, a quien sin derecho aproveche la energía eléctrica, magnética, electromagnética, de cualquier fluido, o de cualquier medio de transmisión, de la persona que legalmente pueda disponer de los mismos.

Artículo 424 bis. Sanciona con 10 años de prisión, a quien produzca, reproduzca y venda en lugares públicos copias de obras, fonogramas, videogramas o libros, protegidos por la Ley Federal del Derecho de Autor, con fin de especulación comercial y sin la autorización del titular de los derechos de autor o de los derechos conexos. Asimismo, a quien fabrique con fin de lucro un dispositivo para desactivar los dispositivos electrónicos de protección de un programa de computación.

Caso 1. Robo de contraseña WIFI

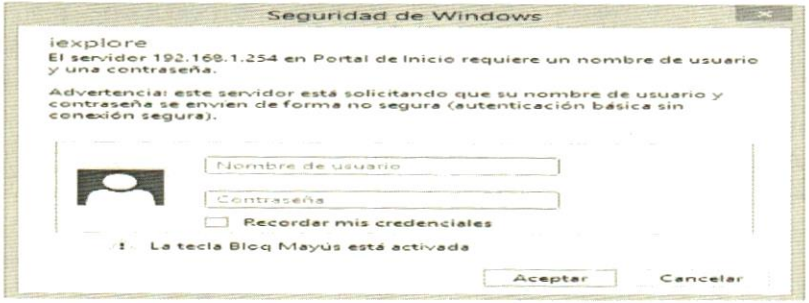
Todos debieran saber que utilizar la red *Wifi* del vecino sin su autorización, es un delito tipificado como robo en el Código Penal Federal, que a la letra dice: Artículo 368. *"Se equiparan al robo y se castigaran como tal: el uso o aprovechamiento de energía eléctrica, magnética, electromagnética, de cualquier fluido, o de cualquier medio de transmisión, sin derecho y consentimiento de la persona que legalmente puede disponer de los mismos"*, pero, ¿qué pasa cuando se enciende un computador y la tarjeta inalámbrica detecta las redes disponibles existentes alrededor? Irónicamente, la invasión de varias señales de redes en los espacios personales, no es delito.

Para entender esta situación de la arquitectura en las conexiones, con apoyo en la ley Federal de Telecomunicaciones, donde destaca el artículo 11 que indica la obligatoriedad de requerir una concesión de la Secretaría para "*instalar, operar o explotar redes públicas de telecomunicaciones*", y el artículo 41 en donde establece que *"los concesionarios de redes públicas de telecomunicaciones deberán adoptar diseños de arquitectura abierta de red para permitir la interconexión e interoperabilidad de sus redes. A tal efecto, la Secretaría elaborará y administrará los planes técnicos fundamentales de numeración, conmutación, señalización, transmisión, tarifación y sincronización, entre otros, a los que deberán sujetarse los concesionarios de redes públicas de telecomunicaciones. Dichos planes deberán considerar los intereses de los usuarios y de los concesionarios"*, de no cumplir con lo previsto el Artículo 71 sancionará de conformidad con la Secretaría con multa de 10,000 a 100,000 salarios mínimos por: *"no cumplir con las obligaciones en materia de operación e interconexión de redes públicas de telecomunicaciones"*. Es por eso que las tarjetas de las computadoras, reconocen redes *WIFI* que están al alcance para establecer una conexión.

Por otra parte, los navegadores y buscadores de *internet*, no están sujetos a ninguna regulación que los responsabilice de la descarga gratuita de programas que obtienen las contraseñas de las redes *Wifi* tras la desencriptación de las claves WEP, WPA y WPA2, tales como: *Beini, Backtrack, Airtrack, Free Wifi y WirelessKeyDump* entre otros, debido a que su uso depende directamente de los intereses de cada persona; es por eso, que se emplean como mecanismos de evaluación a la seguridad inalámbrica o como pruebas de penetración sin restricción alguna.

Una forma de evitar la visibilidad de la red a nivel usuario, consiste en acceder a la página del *Modem* de TELMEX (Teléfonos de México, S.A.B. de C.V.), y registrar el nombre del usuario y la contraseña para desactivar la difusión de la red SSID, *(ver Fig.10).*

Figura 10 .Modem TELMEX



Fuente: [basado de la página de inicio del Modem].

Entonces, ¿Cómo se puede evitar que un niño coma dulces, si se le pone a su alcance un gran tarro de golosinas sin cobertura y destapado?, de la misma manera, puede aplicarse esta analogía al servicio de *internet*, ¿Cómo evitar la sustracción de las contraseñas, sí éstas invaden constantemente la señal, y no se aplica ningún mecanismo de protección?

Mientras la Ley Federal de Telecomunicaciones siga obligando a los concesionarios a tener una arquitectura abierta; los proveedores de *internet* no tengan restricciones en su contenido que incluye la descarga de programas que sirven para obtener las claves de seguridad de redes y los usuarios no se preocupen por bloquear la visibilidad de su red; el robo de contraseñas se convertirá en una actividad cotidiana entre los usuarios de *internet.*

2.2.2. Ley Federal de Telecomunicaciones

Basados en los artículos de esta ley, que tiene como objetivo regular el uso, aprovechamiento y explotación de los concesionarios o permisionarios de las redes de telecomunicaciones, figuran los siguientes:
Artículo 11. Para tener una red pública de telecomunicaciones, es necesario contar con una concesión de la Secretaría.

Artículo 26. El título de concesión contendrá; nombre y domicilio; objeto y servicios; derechos y obligaciones; vigencia; garantía; cobertura geográfica de la red pública.

Artículo 40. Los concesionarios están obligados a colaborar con las autoridades con investigaciones en materia de delincuencia organizada, delitos contra la salud, secuestro, extorsión o amenazas a solicitud del Procurador General de la República, de las entidades federativas o de los servidores públicos en quienes deleguen esta facultad, de conformidad con las leyes correspondientes.

Artículo 41. Los concesionarios de redes públicas deberán adoptar diseños de arquitectura abierta de red para permitir la interconexión e interoperabilidad de sus redes.

Artículo 42. Los concesionarios de redes públicas deberán interconectar sus redes, y a tal efecto suscribirán un convenio, si las "partes" no llegan a un acuerdo, la Secretaría, resolverá sobre las condiciones que no hayan podido convenirse.

Artículo 43. En los convenios de interconexión, las "partes" deberán: identificar los puntos de conexión terminal de su red; permitir el acceso de manera desagregada a servicios, capacidad y funciones de sus redes sobre bases de tarifas no discriminatorias; abstenerse de otorgar descuentos por volumen en las tarifas de interconexión; actuar sobre bases de reciprocidad en la interconexión entre concesionarios que se provean servicios, capacidades o funciones similares entre sí, en tarifas y condiciones; llevar a cabo la interconexión en cualquier punto de conmutación u otros en que sea técnicamente factible.

Artículo 44. Los concesionarios deberán: llevar contabilidad y tener una tarifa asignada por servicios de interconexión; asimismo, un control de la comunicación con los siguientes datos: Tipo de comunicación "voz/datos", servicios "reenvío o transferencia de llamada", tipo de contrato y fecha de activación del servicio, punto de origen y destino, fecha, hora, duración de la comunicación, éstos datos deberán ser resguardados por 12 meses y ser entregados a la procuraduría cuando lo soliciten para facilitar investigaciones de actividades delictivas como la extorsión y el secuestro, de no ser requerido, al finalizar el periodo deberán ser destruidos.

Los concesionarios no deberán: interrumpir el tráfico de señales entre concesionarios interconectados, modificar su red afectando los equipos de los usuarios o de las redes con las que esté interconectada, establecer barreras contractuales o técnicas a la conexión de cableados ubicados dentro del domicilio de un usuario con otros concesionarios de redes públicas.

Artículo 48. Los usuarios de las redes públicas de telecomunicaciones pueden acceder bajo condiciones, a servicios de información, de directorio, de emergencia, de cobro revertido y vía operadora, entre otros.

Artículo 49. La información que se transmita será confidencial, salvo aquella que, por su propia naturaleza, sea pública, o cuando medie orden de autoridad competente.

Artículo 50. La Secretaría procurará redes públicas de telecomunicaciones en todo México, para la atención de servicios públicos y sociales, de la población en general.

Artículo 51. El concesionario de redes públicas de telecomunicaciones que den servicio en localidades, no podrá interrumpir la prestación de dicho servicio, salvo causa de fuerza mayor o que cuente con autorización expresa de la Secretaría.

Artículo 52.- Comercializadora de servicios de telecomunicaciones es aquél que, sin ser propietario de medios de transmisión, proporciona a terceros servicios de telecomunicaciones mediante un concesionario de redes públicas.

Artículo 60. Los concesionarios fijarán libremente las tarifas de los servicios de telecomunicaciones.

Artículo 71. Sanción de 100,000 salarios mínimos por: prestar servicios de telecomunicaciones sin contar con concesión, no cumplir con las obligaciones en materia de operación e interconexión de redes públicas de telecomunicaciones, impedir la actuación de otros concesionarios con derecho a ello, interceptar información que se transmita por las redes públicas de telecomunicaciones, no cumplir el artículo 44 y, sanción de 40,000 salarios mínimos por: operar comercializadoras ilegalmente, Interrumpir el servicio en localidades y cometer errores con los datos de usuarios y en el cobro de los servicios.

Artículo 72. Las personas que presten servicios de telecomunicaciones sin contar con la concesión -artículos 11 y 31-, perderán en beneficio de la Nación los bienes, instalaciones y equipos empleados.

Caso 2. Distribuir internet a una comunidad de usuario

La infraestructura de telecomunicaciones en México no es suficiente para cubrir la demanda de cobertura y penetración de la banda ancha, que se requiere en las zonas urbanas y en algunas zonas rurales de escasos recursos; ante esta necesidad y la flexibilidad que tienen las redes inalámbricas para conectarse, se ha abierto un nuevo mercado de oportunidades, que consiste en la reproducción del servicio de *internet* a terceros en forma irregular.

Para tal efecto, los usuarios con una concesión reproducen el servicio apoyándose de una instalación realizada con puntos de acceso (*Acces point*), con la capacidad de reproducir la señal a una distancia aproximada de 500mts de longitud; éstos pueden ser adquiridos legalmente en cualquier empresa que ofrezca bienes y servicios de telecomunicaciones. Como ejemplo, puede citarse a TELMEX, sin embargo, en el Contrato de Términos y Condiciones, señala dentro la cláusula decima octava "que no está permitido la comercialización, venta o reventa del servicio" y "la conexión del servicio por parte del suscriptor con terceros que se ubiquen fuera del domicilio del suscriptor a través de cualquier tecnología, en el entendido que el suscriptor será responsable de tomar las medidas que sean necesarias para evitar el acceso al servicio a cualquier tercero que no se encuentre dentro del domicilio".

Una de las medidas para incrementar la inclusión social y reducir la brecha digital, estipulado en el artículo 6°, de la Constitución Política de los Estados Unidos Mexicanos, indica que: "El Estado garantizará el derecho de acceso a las tecnologías de la información y comunicación, incluido el de banda ancha e internet"; por medio del "Uso de Internet Libre para Todos" compromiso realizado en el Pacto por México que se basa en las siguientes premisas, citadas en la Reforma en Materia de Telecomunicaciones, (2012):

- Desarrollar una robusta red troncal de telecomunicaciones: se garantiza el crecimiento de la red de CFE, los usos óptimos de las bandas 700MHz y 2.5GHz y el acceso a la banda ancha en sitios públicos bajo el esquema de una red pública del Estado.

- Agenda digital y acceso a banda ancha en edificios públicos: se crea una instancia responsable de la agenda digital que deberá encargarse de garantizar el acceso a *internet* de banda ancha en edificios públicos.

. Otra medida, sería la creación de una comunidad de internautas y ofrecer el servicio en forma legal, en base a las condiciones de servicio de la Comisión del Mercado de las Telecomunicaciones, que por sus siglas se denomina CMT y se rige con las tres condiciones siguientes:

- Sin ánimo de lucro.
- Que la red y el servicio no estén abiertos al público en general,
- Que la prestataria del servicio de atención al cliente sea al operador que celebró el contrato con la concesionaría y no, con los integrantes de la comunidad; citado por Jiménez (2013).

La realidad es que el derecho de navegar por *internet* en sitios públicos y con horarios limitados, no cubre la necesidad de las personas que utilizan el servicio para fines de investigación y difusión del conocimiento, a éstos suelen llamarse usuarios activos, porque bajan y suben información a la red y el ancho de banda no es el indicado.

En México, las comunidades de internautas no aplican, debido a que la CMT es un organismo público regulador independiente de los mercados nacionales de comunicaciones electrónicas y servicios audiovisuales de España.

Por lo tanto, mientras no regulen la venta de los reproductores de señal, y no se fortalezca el servicio de *internet* para todos, la necesidad seguirá siendo una realidad y los prestadores de servicios una solución.

2.2.3. Ley Federal del Derecho de Autor

Basados en los artículos de la Ley Federal del Derecho de Autor, (2013), que tiene por objetivo regular los derechos del autor sobre sus obras, sobresalen:

Artículo 3. Las obras protegidas por esta Ley son aquellas de creación original susceptibles de ser divulgadas o reproducidas en cualquier forma o medio.

Artículo 29. Los derechos patrimoniales estarán vigentes durante la vida del autor y, a partir de su muerte, cien años más.

Artículo 101. Se entiende por programa de computación como un conjunto de instrucciones estructuradas, que tiene como propósito que una computadora o dispositivo realice una función específica.

Artículo 102.- Los programas de computación operativos y aplicativos, se protegen en los mismos términos que las obras literarias. Se exceptúan aquellos que tengan por objeto causar daño a otros programas o equipos.

Artículo 103.- Salvo pacto en contrario, los derechos patrimoniales sobre un programa de computación y su documentación, cuando hayan sido creados por uno o varios empleados en el ejercicio de sus funciones, corresponden a éste. Como excepción a lo previsto por el artículo 33 de la presente Ley, el plazo de la cesión de derechos en materia de programas de computación no está sujeto a limitación alguna.

Artículo 104.- Como excepción a lo previsto en el artículo 27 fracción IV, el titular de los derechos de autor sobre un programa o una base de datos conservará, aún después de la venta de ejemplares, el derecho de autorizar o prohibir el arrendamiento de dichos ejemplares. Este precepto no se aplicará cuando el ejemplar del programa de computación no constituya en sí mismo un objeto esencial de la licencia de uso.

Artículo 105.- El usuario legítimo de un programa de computación podrá realizar el número de copias que le autorice la licencia concedida por el titular de los derechos de autor, o una sola copia de dicho programa siempre y cuando: sea indispensable para la utilización del programa, o como resguardo para sustituir la copia legítimamente adquirida, la copia de respaldo deberá ser destruida cuando cese el derecho del usuario para utilizar el programa de computación.

Artículo 106.- El derecho patrimonial sobre un programa de computación comprende la facultad de autorizar o prohibir: la reproducción del programa, por cualquier medio y forma; la traducción, la adaptación o modificación de un programa y la reproducción del programa resultante; la distribución y alquiler del programa; la decompilación y el desensamblaje del programa.

Artículo 107. Las bases de datos que por razones de disposición de su contenido constituyan creaciones intelectuales, quedarán protegidas como compilaciones. Dicha protección no se extenderá a los datos y materiales en sí mismos.

Artículo 108.Las bases de datos que no sean originales quedan, protegidas en su uso exclusivo por quien las haya elaborado, durante un lapso de 5 años.

Artículo 109. El acceso a información de carácter privado de las personas, contenida en las bases de datos, así como la publicación, reproducción, divulgación, comunicación pública y transmisión de dicha información, requerirá la autorización previa de las personas de que se trate, en excepto si se trata de autoridades autorizadas por ley.

Artículo 110. El titular del derecho patrimonial sobre una base de datos tendrá el derecho exclusivo, de autorizar o prohibir: Su reproducción por cualquier medio y de cualquier forma; su traducción, adaptación, reordenación y modificación; su distribución del original o copias de la base de datos y su comunicación al público.

Artículo 111.- Los programas efectuados electrónicamente que contengan elementos visuales, sonoros, tridimensionales o animados quedan protegidos por esta Ley en los elementos primigenios que contengan.

Artículo 112.- Queda prohibida la importación, fabricación, distribución y utilización de aparatos o la prestación de servicios destinados a eliminar la protección técnica de los programas de cómputo, de las transmisiones a través del espectro electromagnético y de redes de telecomunicaciones y de los programas de elementos electrónicos señalados en el artículo anterior.

Artículo 113.- Las obras e interpretaciones o ejecuciones transmitidas por medios electrónicos a través del espectro electromagnético y de redes de telecomunicaciones y el resultado que se obtenga de esta transmisión estarán protegidas por esta Ley.

Artículo 164. El Registro Público del Derecho de Autor tiene las siguientes obligaciones: Inscribir obras y brindar información de las inscripciones cuando sea solicitada. Tratándose de programas de computación, la obtención de copias sólo se permitirá mediante autorización del titular del derecho patrimonial o por mandamiento judicial.

Caso 3. Licencias de software Copyrigth & Copyleft

El titular de los derechos de autor de un programa, es aquella persona física o moral que puede usar, reproducir, distribuir, difundir la obra registrada,

según el artículo 27 de la Ley de Derechos de Autor (2013); siempre y cuando los programas de aplicación u operativos creados no sean dañinos en la ejecución de otros programas o equipos, basados en el artículo 102 de la misma ley.

Ejemplo: ***Copyrigth & Copyleft***

Cuando se aluden los términos *Copyrigth y Copyleft*, inmediatamente se relacionan con *software* propietario y *software* libre; debido a la filosofía de sus autores sobre el uso, distribución, difusión y reproducción limitada o ilimitada; y sobre el beneficio económico que se pueda obtener por su adquisición; pero en el papel de usuario, no se debe perder el punto de vista del titular de la obra porque los derechos adquiridos por cualquier opción son heredables o trasmitidos.

El *software* propietario es común relacionarlo con "oneroso" y el *software* libre con "gratuito"; pero no es lo correcto, porque existen programas operativos y de aplicación de ambas clasificaciones que se pueden *comprar o adquirir sin costo alguno*. Para confirmar lo anterior, se mencionan a dos grandes compañías como representantes del *Copyrigth*: Google Inc. y Microsoft Corp., que ofrecen gratuitamente sus buscadores en línea: *Google y Bing*, y programas de aplicación, tales como: *Google earth o gmail y Skype*; pero también son reconocidos por vender sus programas a nivel nacional e internacional, un ejemplo de ello serían los sistemas operativos: *Android y Windows*, que han logrado posicionarse en el agrado del público.

De la misma manera dentro del *software* libre como representante principal del *Copyleft*, sobresalen: al Navegador *Firefox* de *Mozilla*, al sistema operativo *Ubuntu* de *Linux*, a los programas de aplicación: *Open Office y OpenAudit*, y a los administradores de base de datos *MySql* y *Postgres*, todos ellos con distribución gratuita; en el caso de los programas que requieren una licencia que implica un gasto económico se señala al sistema operativo *Red Hat Entreprise* de *Linux*.

En forma especial se mencionan a todos los programas Apache XML, AXIS y otros que siendo que siendo *software* libre, tienen un aviso *copyright*, pero es compatible con la licencia pública general, o mejor conocida por sus siglas en inglés GPL.

Entonces, surgen las siguientes interrogantes:

¿El Copyrigth es exclusivo para los software propietario?, la respuesta sería No, porque el registro del programa, depende directamente del titular de la obra.

¿El Copyleft protege la comercialización de los programas?, la respuesta sería Sí, pero todo depende de los derechos estipulados por el autor, al momento de tramita las licencias GPL o *Creative Commons*.

¿Las licencias CopyLeft son reconocidas en el marco legal de México? Aunque las condiciones de la licencia son muy claras, existe conflicto para dictaminar si ha ocurrido un delito, porque el aviso de notificación *copyright* en el programa puede ser alterado fácilmente y el registro que reconoce la Fundación de *Software* Libre (FSF) puede omitir algunos detalles por los problemas de traducción al español.

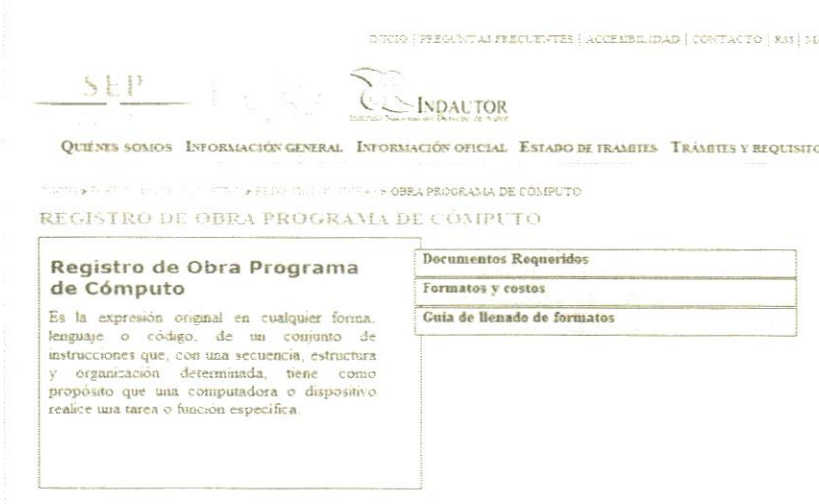
Por lo tanto, las licencias *Copyleft* son reconocidas pero no pueden avalarse jurídicamente en su totalidad.

Con la finalidad de un mayor entendimiento, se presenta información adicional:

1. Instituto Nacional del Derecho de Autor

Por sus siglas se le conoce como INDAUTOR y es una Institución adscrita a la Subsecretaria de Educación Superior de la Secretaría de Educación Pública encargada de proteger y fomentar los derechos de autor por medio del registro de obras, contratos de cesión y licencias de uso; asimismo del Número Internacional Normalizado del Libro denominado ISBN aplicado a los programas de cómputo; A continuación se presenta la pantalla principal del Instituto para el trámite del registro *(ver Fig.11)*.

Figura 11. Registro INDAUTOR



Fuente: [basado de la página, INDAUTOR].

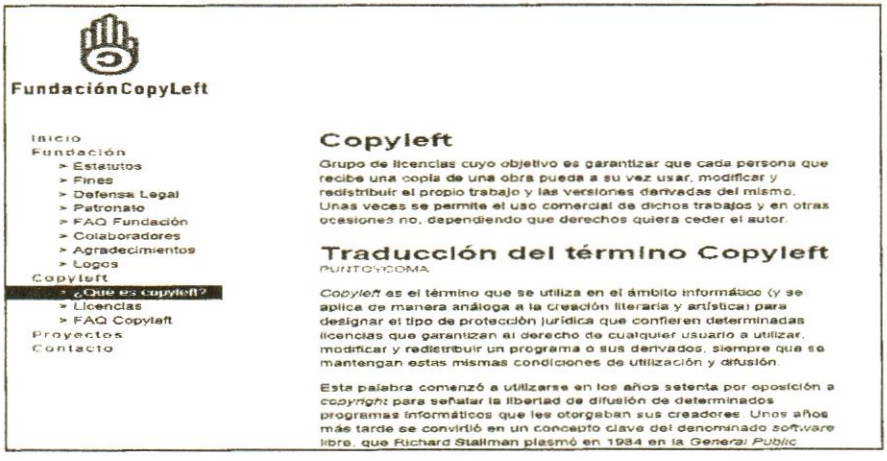
2. *Copyleft*

Es un término que se usa en el área de informática para designar el tipo de protección jurídica por medio de las licencias: *GPL, Creative Commons, Coloriuris,* Aire Incondicional y Arte Libre.

Su objetivo es otorgar el derecho a cualquier usuario de utilizar, modificar y redistribuir un programa, siempre y cuando se mantengan la misma condición de utilización y distribución.

Se aprecia en la siguiente imagen los estatutos, fines, defensa legal, patronato, colaboradores, agradecimientos y logos de la fundación, asimismo, la definición y licencias de *Copyleft, (ver Fig.12).*

Figura 12. Fundación *CopyLeft*



Fuente: [basado de la página, Fundación *Copyleft*]

3. Licencia Pública General GPL

Es una Licencia Pública General que garantiza la legalidad de usar, modificar y distribuir un programa gratuitamente u onerosamente, la forma correcta de establecerlo es anotar en la cabecera de cada fichero un aviso informativo del *copyrigth* y una autorización otorgada a los usuarios para distribuir el código bajo los términos GPL, como a continuación se describe:

```
# Título del programa
# Titular de la obra
# Copyright (C) año de creación
# Este programa no tiene restricción para ser
usado, modificado y/o
# distribuido.
```

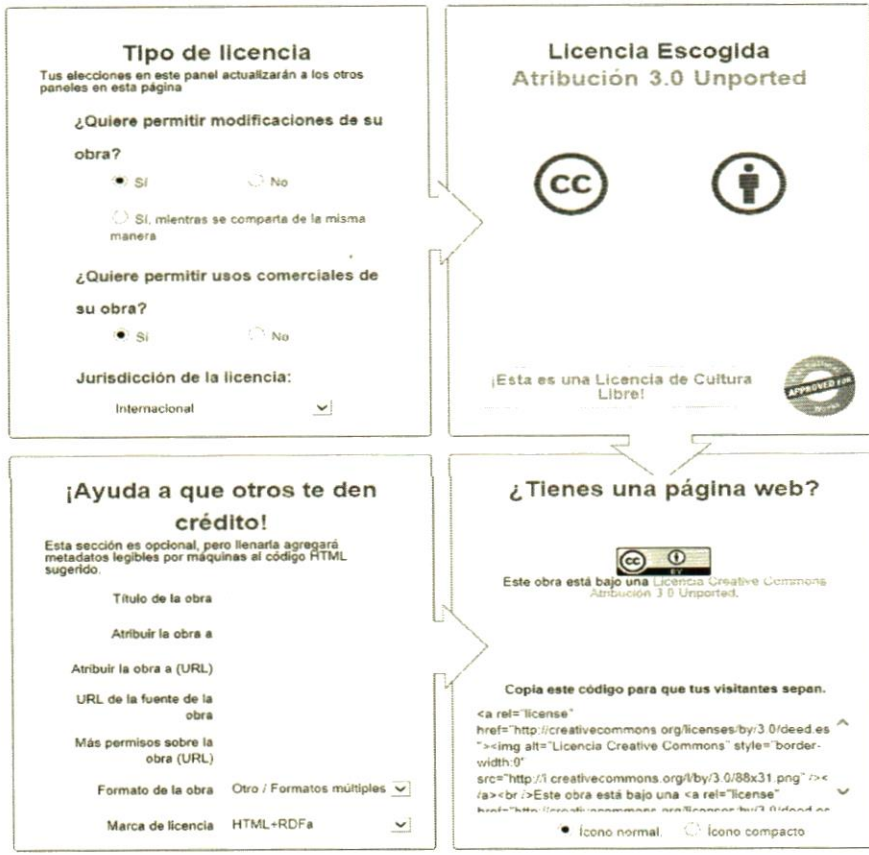
4. Licencia *Creative Commons*

Están basadas en el marco jurídico de Estados Unidos y es un proyecto que cuenta con la participación de Brasil, Finlandia y Japón y posteriormente se incorpora España. Por otra parte, estas licencias han tomado gran auge para proteger los derechos de los autores de Páginas *Web*; que permitan a los usuarios crear, usar, reproducir, difundir y/o realizar obras derivadas con la condición de reconocer públicamente los créditos del titular, no obtener

ningún beneficio económico, y no realizar obras derivadas; en caso contrario la obra creada a partir de la transformación, será sujeta a la misma licencia.

Para obtener una licencia, solo es necesario ingresar al sitio *web* y contestar correctamente los formularios (*ver Fig.13).*

Figura 13. CREATIVE COMMONS



Fuente: [basado en la página, *Creative Commons*]

2.2.4. Ley de la Propiedad Industrial

Basados en los artículos de la Ley de la Propiedad Industrial, (2012), que tiene por objetivo proteger los derechos de marcas y patentes, destacan:

Artículo 2. Esta ley tienen por objeto: Proteger la propiedad industrial mediante la regulación y otorgamiento de patentes de invención; registros de modelos de utilidad, diseños industriales, marcas, y avisos comerciales; publicación de nombres comerciales; declaración de protección de denominaciones de origen, y regulación de secretos industriales.

Artículo 6. El Instituto Mexicano de la Propiedad Industrial, tiene la facultad de otorgar patentes de invención, y registros de modelos de utilidad, diseños industriales, marcas, y avisos comerciales, emitir fama de marcas; publicar nombres comerciales, inscripciones, renovaciones, transmisiones de licencias de uso y explotación.

Artículo 19. Los programas de cómputo no se consideran invenciones

Artículo 32. Los diseños industriales de un producto con fines de representación que le den al producto un aspecto peculiar, son los dibujos formados por figuras, líneas o colores.

Artículo 63. El titular de la patente podrá conceder, mediante convenio, licencia para su explotación, misma que deberá ser inscrita en el Instituto para su validez.

Artículo 82. Secreto industrial es la información de aplicación industrial o comercial que guarde una persona física o moral con carácter confidencial, que le signifique obtener o mantener una ventaja competitiva o económica frente a terceros en la realización de actividades económicas y respecto de la cual haya adoptado los medios o sistemas suficientes para preservar su confidencialidad y el acceso restringido a la misma.

Artículo 87. Los industriales, comerciantes o prestadores de servicios podrán hacer uso de marcas. Sin embargo, el derecho a su uso exclusivo se obtiene mediante su registro en el Instituto.

Artículo 88. Se entiende por marca a todo signo visible que distinga productos o servicios de otros de su misma especie o clase en el mercado.

Artículo 89. Una marca puede ser: Las denominaciones y figuras visibles, Las formas tridimensionales; los nombres comerciales y el nombre propio de una persona física, siempre que no se confunda con una marca registrada o un nombre comercial publicado.

Artículo 90. No pueden ser marcas: Las denominaciones, figuras o formas tridimensionales que sean descriptivas de los productos o servicios; que reproduzcan o imiten, sin autorización, escudos, banderas o emblemas de cualquier país, estado, municipio o divisiones políticas equivalentes, así como las denominaciones, siglas, símbolos o emblemas de organizaciones internacionales, gubernamentales, no gubernamentales o de cualquier otra organización reconocida oficialmente, así como la designación verbal de los mismos; que sea idéntica o semejante en grado de confusión a otra en trámite de registro presentada con anterioridad o a una registrada y vigente, aplicada a los mismos o similares productos o servicios. Sin embargo, sí podrá registrarse una marca que sea idéntica a otra ya registrada, si la solicitud es planteada por el mismo titular.

Artículo 98 bis. Una marca es notoriamente conocida en México, cuando un sector determinado del público o de los círculos comerciales del país, conoce la marca como consecuencia de las actividades comerciales desarrolladas en México o en el extranjero, como consecuencia de la promoción o publicidad de la misma

Artículo 99. El derecho exclusivo para usar un aviso comercial se obtendrá mediante su registro ante el Instituto.

Artículo 100- Se considera aviso comercial a las frases u oraciones que tengan por objeto anunciar al público establecimientos o negociaciones.

Artículo 213. Infracciones administrativas:

- Ofrecer productos o procesos sin licencia, registro o patente.
- Usar una marca, nombre comercial o aviso comercial parecido a otro registrado, para amparar los mismos o similares productos o servicios que los protegidos; sin el consentimiento manifestado por escrito del titular.
- Causar confusión al público al suponer infundadamente que existe una relación entre las actividades comerciales o mercantiles, del establecimiento con que ofrece los mismos productos o servicios, pero con licencia.

- Reproducir y distribuir un esquema de trazado protegido, sin la autorización del titular del registro, en su totalidad o cualquier parte que se considere original por sí sola, aún sea por incorporación en un circuito integrado o en otra forma.

Artículo 214. Las infracciones administrativas a esta Ley, serán sancionadas con multas, clausuras o arresto.

Artículo 218. En los casos de reincidencia se duplicarán las multas impuestas anteriormente, sin que su monto exceda del triple del máximo fijado en el artículo 214 de esta Ley.

Caso 4. Usurpación de marcas patentadas

Uno de los principales retos de los creadores de servicios y productos es registrar su marca, nombre comercial o aviso comercial ante el Instituto Mexicano de la Propiedad Industrial (IMPI), para asegurarse de tener derecho exclusivo de su uso y explotación, sin embargo existen situaciones en que otras personas físicas o morales emplean el mismo o similar producto o servicio patentado de forma dolosa.

Ejemplo: ***Iphone demanda a IFone***

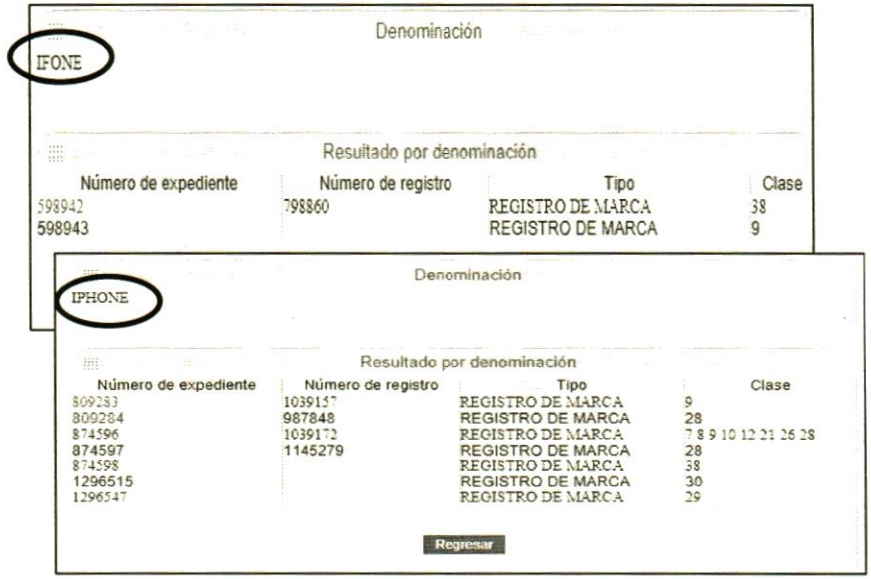
IFone, S.A. de C.V. es una empresa mexicana que ofrece y comercializa productos y servicios de telecomunicaciones de la empresa AltiGen Comunications Inc., que en el año 2009 fue demandada por el gigante *Apple, por la confusión fonética que puede ocasionar el pronunciamiento de ambas marcas por el público. (Ver Fig.14).*

Figura 14. Ifone vs Iphone

Fuente: [basado en (Graniel, 2014)]

En vano ha sido el esfuerzo de la compañía Apple de registrar su marca ante el Instituto Mexicano de la Propiedad Industrial, cuando en el 2007 se le notificó que su solicitud no era aceptable por que ya existía una marca semejante que ocasionaría confusión, registrada en Junio de 2003 en el Banco Nacional de Marcas, denominado por sus siglas como MARCANET, *(ver Fig. 15)*.

Figura 15. MARCANET



Fuente: [basado en el servicio de consulta externa, MARCANET]

Esta resolución, está basada en el artículo 89 y 90 de la Ley de la Propiedad Industrial, que indica *"...la designación verbal de los mismos; que sea idéntica o semejante en grado de confusión a otra en trámite de registro presentada con anterioridad o a una registrada y vigente, aplicada a los mismos o similares productos o servicios..."*

Nuevamente, con el ánimo de ganar *iPhone Apple* demanda a *iFone,* basándose al Artículo 98 de la misma Ley, donde argumenta *que "es una marca no reconocida notoriamente en México*"; querella que vuelve a perder ante la lista de clientes, empleados y estados financieros que se presentan en el tribunal, como último recurso interpone una demanda de caducidad pronunciando que la marca *IFone* no se había usado por más tres años

consecutivos; como respuesta es contrademandado junto con las compañías telefónicas *Telcel, Movistar* y *Iusacel* por posible invasión de marca y daños colaterales; (Onofre, 2013).

Entre las sanciones adjudicadas a *iPhone*, se contempla una indemnización económica por concepto de daños y perjuicios, y una multa a las principales compañías de telefonía móvil en el país.

Finalmente seis años después, IMPI dictamina a favor de *Ifone* sancionando y prohibiendo a las tres compañías el uso de la marca, asimismo, anula la demanda de la empresa extranjera y la contrademanda de la empresa mexicana argumentando que *Iphone* solo comercializa *Smartphone*, y no ofrece servicios de telecomunicaciones, como: telefonía, multimedia e *internet*; citado por Michel, (2014). Por lo tanto se autoriza el registro de la patente a la empresa *Apple* en la clase 9, que respalda la comercialización del aparato y niega el registro en la clase 38, que integra servicio de telefonía, multimedia e *internet*.

Entonces, ¿Por qué en México se presentan casos como el descrito?, ¿Qué ocurre con el marco jurídico?

La usurpación de marcas patentadas, siempre será una acción penada en el país; pero una forma de exentar o aplazar la sanción, dependerá de la forma dolosa o imprudencial en que se registra el producto.

Para mayor conocimiento, se presenta a continuación el expediente 809283 de *iPhone* con los datos del registro y la imagen con la descripción de la clase *(ver Fig. 16):*

- Datos Generales: Fecha de concesión: 07/05/2008, Fecha de vigencia: 27/09/2016, Tipo de solicitud: Marca y Tipo de Marca: Nominativa.

- Descripción del producto: "Dispositivo electrónico digital móvil para el envío y recepción de llamadas telefónicas (transmisión de voz), correos electrónicos y otros datos digitales, reproductores de música digital MP3 y otros reproductores de formato de audio digital; asistentes personales, organizadores electrónicos, agendas electrónicas, teléfonos celulares, cámaras y programas de computadoras para navegar y buscar bases de datos en línea".

- Datos del Titular: Nombre: Apple Inc., País: Estados Unidos de América

Figura 16. MARCANET_Registro

Productos y servicios

Clase	Tipo de clase	Descripción
9	8	DISPOSITIVOS ELECTRONICOS DIGITALES MOVILES PARA EL ENVIO Y RECEPCION DE LLAMADAS TELEFONICAS (TRANSMISION DE VOZ), CORREOS ELECTRONICOS, Y OTROS DATOS DIGITALES; REPRODUCTORES DE MUSICA DIGITAL (MP3) Y OTROS REPRODUCTORES DE FORMATO DE AUDIO DIGITAL; ASISTENTES PERSONALES DIGITALES, ORGANIZADORES ELECTRONICOS, AGENDAS ELECTRONICAS, TELEFONOS CELULARES, CAMARAS, PROGRAMAS DE COMPUTADORA PARA ACCESAR, NAVEGAR Y BUSCAR EN BASES DE DATOS EN LINEA.

Fuente: [basado en el servicio de consulta en línea, MARCANET]

Otro mecanismo de consulta sería las bases de datos registradas en el Buscador de Patentes en México, conocido también como INFOPAT *(ver Fig. 17)*.

Figura 17. INFOPAT

Fuente: [basado en el servicio de consulta en línea, INFOPAT]

- El Resultado de Patentes Concedidas: 223 [1-20]
- Frase buscada: Teléfono Móvil
- Patente: MX 16756
- Título: Modelo Industrial de Teléfono móvil

Ambas páginas relacionadas con el instituto Mexicano de la Propiedad Industrial *(ver Fig. 18)*, que ofrece el servicio gratuito de los registros de las marcas y patentes, y las cotizaciones por cada trámite.

Figura 18. IMPI Servicios

Fuente: [basado en el servicio en línea, IMPI]

Además incluye los servicios siguientes:

- Sistema de Información de la Gaceta de la Propiedad Industrial (SIGA)
- Tarifas de Servicios del IMPI
- Formatos
- Cursos y Talleres
- Servicios Electrónicos

2.2.5. Ley Federal de Protección al Consumidor

La Ley Federal de Protección al Consumidor, (2013), tiene por objetivo regular la relación consumidor y proveedor, establece los siguientes ordenamientos relacionados:

Artículo 1. El objeto de esta ley es promover y proteger los derechos y cultura del consumidor y procurar la equidad, certeza y seguridad jurídica en las relaciones entre proveedores y consumidores.

Artículo 5. Quedan excluidos los servicios regulados por las leyes financieras que presten las Instituciones y Organizaciones cuya supervisión esté a cargo de las comisiones nacionales Bancaria y de Valores; de Seguros y Fianzas; del Sistema de Ahorro para el Retiro o de cualquier órgano de regulación dependiente de la Secretaría de Hacienda y Crédito Público.

Artículo 16.- Los proveedores y empresas que utilicen información sobre consumidores con fines mercadotécnicos o publicitarios están obligados a informar gratuitamente a la persona que lo solicite si mantienen información acerca de ella.

Artículo 66.- En toda operación a crédito al consumidor, se deberá:

- Informar al consumidor previamente sobre el precio de contado del bien o servicio de que se trate, el monto y detalle de cualquier cargo si lo hubiera, el número de pagos a realizar, su periodicidad, el derecho que tiene a liquidar anticipadamente el crédito con la consiguiente reducción de intereses, en cuyo caso no se le podrán hacer más cargos que los de renegociación del crédito, si la hubiere. Los intereses, incluidos los moratorios, se calcularán conforme a una tasa de interés fija o variable;
- ...En caso de haberse efectuado la operación, el proveedor deberá enviar al consumidor al menos un estado de cuenta bimestral, por el medio que éste elija, que contenga la información relativa a cargos, pagos, intereses y comisiones, entre otros rubros.

Artículo 76 BIS. En las relaciones entre proveedores y consumidores en las transacciones efectuadas a través del uso de medios electrónicos, ópticos o de cualquier otra tecnología.

- El proveedor utilizará la información proporcionada por el consumidor en forma confidencial, por lo que no podrá difundirla o transmitirla a otros proveedores ajenos a la transacción, salvo autorización expresa del propio consumidor o por requerimiento de autoridad competente;
- El proveedor utilizará elementos técnicos para brindar seguridad y confidencialidad a la información proporcionada por el consumidor e informará a éste, previamente a la celebración de la transacción, de las características generales de dichos elementos;
- III. El proveedor deberá proporcionar al consumidor, antes de celebrar la transacción, su domicilio físico, números telefónicos y demás medios a los que pueda acudir el propio consumidor para presentarle sus reclamaciones o solicitarle aclaraciones;
- IV. El proveedor evitará las prácticas comerciales engañosas respecto de las características de los productos, por lo que deberá cumplir con las disposiciones relativas a la información y publicidad de los bienes y servicios que ofrezca, señaladas en esta Ley y demás disposiciones que se deriven de ella;
- V. El consumidor tendrá derecho a conocer toda la información sobre los términos, condiciones, costos, cargos adicionales, en su caso, formas de pago de los bienes y servicios ofrecidos por el proveedor.

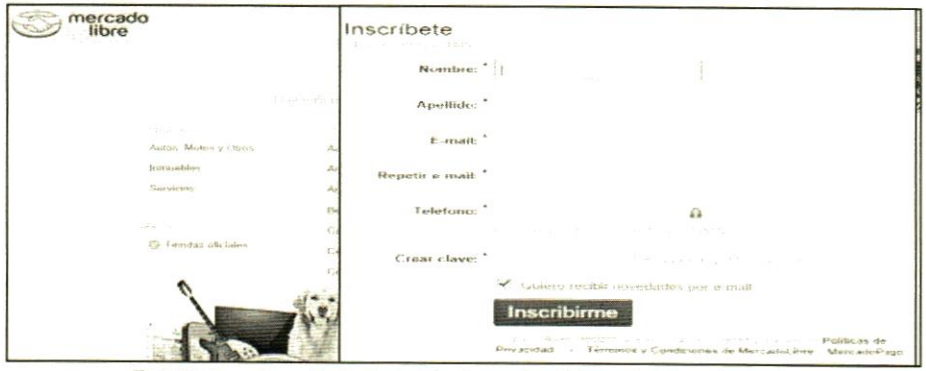
Caso 5. Fraude en Páginas de ventas por Internet

Muchos cibernautas acostumbran a navegar en distintas páginas; ingresan a las mismas realizando operaciones en línea con la confianza de estar respaldados por la compañía, pero en algunas ocasiones el riesgo de fraude se convierte en amenaza, y es precisamente cuando debe analizarse sí la protección que se brinda a los consumidores, es adecuada.

Mercado Libre es una de las páginas de mayor preferencia para miles de usuarios mexicanos por la facilidad y seguridad que ofrecen sus transacciones de venta y compra de productos y servicios en línea *(ver Fig. 19)*, además de inmuebles y transporte.

Para poder realizar una operación los usuarios deben de estar previamente registrados en el sistema y haber aportado datos personales como son: el nombre, apellido, *e-mail* y teléfono, además de aceptar los Términos y Condiciones del uso del sitio y estar acuerdo con el aviso de privacidad. Practica que la mayoría de los usuarios realiza sin detenerse a leer el Contrato.

Figura 19. Mercado Libre



Fuente: [basado en Contrato de Términos y Condiciones de Mercado Libre]

A continuación se presentan de manera concreta, los puntos más relevantes del Contrato de Términos y Condiciones de Mercado Libre, (2012):

- **Inscripción.** L*a veracidad de los datos personales es responsabilidad del usuario*, así también la confidencialidad de la clave de seguridad y seudónimos. La cancelación de cuenta se produce en el caso que se detecten duplicidad en la misma. Las operaciones realizadas con una cuenta, es responsabilidad del usuario y es obligación del mismo reportar el manejo no autorizado.
- **Obligaciones.** Es obligación del comprador contactar al vendedor o viceversa para cerrar la venta. El comprador debe exigir un comprobante de pago, pero el vendedor no está obligado a emitir factura o *ticket*, solo en el caso que sea persona física. La venta puede cancelarse al no comprobar la identidad en alguna de ambas partes. *El sitio no es responsable por el incumplimiento de la venta de artículos*, ni de las obligaciones fiscales.
- **Sanciones.** *El sitio podrá suspender temporal o definitivamente una cuenta* y sancionar a un usuario si no cumple con el presente contrato, *si realiza actos fraudulentos o proporciona datos que imposibiliten verificar su identidad*, removerá los artículos del sitio y no devolverá el importe del servicio de la publicación.
- **Responsabilidad**. El sitio solo ofrece un espacio virtual para realizar transacciones de compra y venta de artículos. *El usuario asume el riesgo de realizar operaciones con terceros que puedan ser menores de edad o tengan una identidad falsa. Los reclamos o acciones legales, eximen de toda responsabilidad al sitio y a su personal correspondiente*.

- **Alcance.** Este contrato no crea ninguna sociedad. *El sitio no tiene el control de la operación ni de los artículos y no garantiza la veracidad de los datos personales*, ni de la publicidad.
- **Indemnización**. El usuario indemnizará al sitio *por cualquier demanda de otros usuarios* por su incumplimiento a este contrato o por la violación de los derechos de terceros.
- **Jurisdicción**. Este contrato está regido por leyes mexicanas, en particular contratación electrónica y comercio electrónico. Cualquier controversia será sometido a los tribunales correspondientes.

Al término de la lectura pueden plantearse las siguientes interrogantes:

¿Porque el sitio de *internet* no asume el compromiso del cumplimiento de las transacciones?

¿Cómo afecta al consumidor la falta de veracidad de los datos de personales?

¿Qué acciones se deben de realizar cuando una transacción de compra-venta no culmina exitosamente por causa de acciones dolosas o fraudulentas, originadas por uno de los dos usuarios involucrados?

Por lo anterior, "se considera conveniente adecuar el marco jurídico mexicano con relación al Código Civil Federal, Código de Comercio y Ley Federal de Protección; para conceder efectos jurídicos a la información electrónica, para dar seguridad jurídica a los comerciantes en el uso de medios electrónicos, para proteger los derechos de los consumidores en la operaciones electrónicas efectuadas, y lograr la interacción global e integral de los campos en que se utilizan los medios electrónicos", basados en (López Varas, 2010).

Cuando se aplica el Código de Comercio, (2014) en las actividades comerciales, nos enfocaremos al Título II, Capítulo I y II, con el objetivo de garantizar que la información recibida o enviada través de mensaje de datos electrónicos son confiables y tiene la misma figura jurídica, que los datos recabados manualmente; asimismo, asegura que la firma electrónica tiene las mismas obligaciones y responsabilidades legales que la firma autógrafa.

2.2.6. Ley Federal de Protección de Datos Personales en Posesión de Particulares

Basados en los artículos de la Ley Federal de Protección de Datos Personales en Posesión de Particulares, (2010), cuyo objetivo es proteger los derechos de los titulares; figuran:

Artículo 3. Para los efectos de esta Ley, se entenderá por:

- I. Aviso de Privacidad: Documento físico o electrónico generado por el responsable que es puesto a disposición del titular.
- VI. Datos personales sensibles: Aquellos que puedan revelar aspectos como origen racial o étnico, estado de salud, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual.

Artículo 7. Los datos personales deberán recabarse y tratarse de manera lícita, no a través de medios engañosos o fraudulentos.

Artículo 9. No podrán crearse bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas.

Artículo 12. El tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades previstas en el aviso de privacidad.

Artículo 16. El aviso de privacidad deberá contener, al menos, la siguiente información:

- I. La identidad y domicilio del responsable que los recaba;
- II. Las finalidades del tratamiento de datos;
- III. Las opciones y medios que el responsable ofrezca a los titulares para limitar el uso o divulgación de los datos;
- IV. Los medios para ejercer los derechos de acceso, rectificación, cancelación u oposición, de conformidad con lo dispuesto en esta Ley;
- V. En su caso, las transferencias de datos que se efectúen, y
- VI. El procedimiento y medio por el cual el responsable comunicará a los titulares de cambios al aviso de privacidad, de conformidad con lo previsto en esta Ley.

El aviso de privacidad deberá señalar expresamente, sí se trata de datos sensibles.

Artículo 19. Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad que permitan proteger los datos personales contra daño, pérdida, alteración o tratamiento no autorizado.

Artículo 21. El responsable o terceros que intervengan en cualquier fase del tratamiento de datos personales deberán guardar confidencialidad respecto de éstos, obligación que subsistirá aun después de finalizar sus relaciones con el titular o, en su caso, con el responsable.

Artículo 63.- Constituyen infracciones a esta Ley, las siguientes conductas llevadas a cabo por el responsable:

I. No cumplir con la solicitud del titular para el acceso, rectificación, cancelación u oposición al tratamiento de sus datos personales, sin razón fundada, en los términos previstos en esta Ley;
II. Actuar con negligencia o dolo en respuesta de solicitudes de acceso, rectificación, cancelación u oposición de datos personales;
III. Declarar dolosamente la inexistencia de datos personales;
IV. Dar tratamiento a los datos personales en contravención a los principios establecidos en la presente Ley;
V. Omitir en el aviso de privacidad, alguno o todos los elementos a que se refiere el artículo 16 de esta Ley;
VI. No efectuar las rectificaciones o cancelaciones de los datos, que legalmente procedan cuando resulten afectados los derechos de los titulares;
VII. No cumplir con el apercibimiento a que se refiere la fracción I del artículo 64;
VIII. Incumplir el deber de confidencialidad.
IX. Cambiar sustancialmente la finalidad originaria del tratamiento de los datos.
X. Transferir datos a terceros sin comunicar a éstos el aviso de privacidad que contiene las limitaciones a que el titular sujetó la divulgación de los mismos;
XI. Vulnerar la seguridad de bases de datos, locales, programas o equipos, cuando resulte imputable al responsable;
XII. Llevar a cabo la transferencia o cesión de los datos personales, fuera de los casos en que esté permitida por la Ley;
XIII. Recabar o transferir datos personales sin el consentimiento expreso del titular, en los casos en que éste sea exigible;
XV. Recabar datos en forma engañosa y fraudulenta;
XVIII. Crear bases de datos en contravención a lo dispuesto por el artículo 9, segundo párrafo de esta Ley.

Artículo 67. Se impondrán de tres meses a tres años de prisión al que estando autorizado para tratar datos personales, con ánimo de lucro, provoque una vulneración de seguridad a las bases de datos bajo su custodia.

Artículo 68. Se sancionará con prisión de seis meses a cinco años al que, con el fin de alcanzar un lucro indebido, trate datos personales mediante el engaño, aprovechándose del error en que se encuentre el titular o la persona autorizada para transmitirlos.

Caso 6. Servicio telefónico al cliente vía telefónica

Call Center de México es una organización con más de 1,200 estaciones de trabajo instaladas con la más alta tecnología y más de 2,000 colaboradores especializados que se comunican vía telefónica con los consumidores de varias empresas, para conocer su opinión sobre el servicio al cliente, para ofrecerles productos o servicios en venta y para otorgarles el mejor soporte técnico de asistencia en línea, basados en información de (Call Center). *(Ver Fig. 20).*

Figura 20. Call Center México

Fuente: [basado en servicios en línea, Call Center México]

Uno de los requisitos principales para brindar una atención personalizada a los clientes o usuarios de los servicios es tener de cada uno sus datos personales; los cuales son proporcionados por parte de las empresas a los centros de atención telefónica en grandes bases de datos controladas por normas de seguridad. Entre los mecanismos y medidas de control que se aplican en el país puede mencionarse al Instituto Federal de Acceso a la Información y Protección de Datos (IFAI) que tiene como función garantizar la debida protección y confidencialidad de los mismos; así también, como requisito legal las empresas que ofertan bienes y servicios deben incluir en los términos y condiciones de su contrato el Aviso de Privacidad sobre el tratamiento de los datos personales para dar cumplimiento al marco jurídico mexicano; en este caso, de manera específica se refiere a la Ley Federal de Protección de Datos Personales en Posesión de Particulares.

Cuando se alude a los fraudes telefónicos, se refiere a una llamada realizada entre un estafador y una víctima, que a través del engaño, proporciona información falsa sobre una empresa, un producto o un servicio, con la finalidad de realizar una transacción y obtener un beneficio económico a favor del delincuente, que rara vez será reembolsado, al momento de denunciar el acto ilícito.

Otra modalidad es el contrato de servicios y adquisición de productos adquiridos sin el consentimiento del consumidor pero con grabaciones de autorización, esta opción puede ser más elaborada y emplear archivos de audio, con la voz de las personas legalmente identificadas pero editadas con respuestas predeterminadas.

Cuando esto ocurre, no hay manera de corroborar el origen de la llamada ni mucho menos la identidad de la persona al otro lado de la línea, pero lo más delicado es ignorar que se han convertido en propietarios de los datos personales; como: nombre completo, dirección, edad, lugar de trabajo, afiliación al sindicato, nombre del esposo y de los hijos, cuentas de tiendas departamentales, cuentas bancarias, créditos bancarios de autofinanciamiento o de hipoteca a la vivienda, afiliación a un centro de recreación, preferencia política, religión, salud y muchos más; y que pueden emplearlos en cualquier momento, dejando vulnerables a sus potenciales clientes, de las acciones que emprendan posteriormente.

2.3. Normas Extranjeras

2.3.1. *Ley Sarbanes Oxley* (SOX)

Su título completo es *Sarbanes-Oxley Act of*, se crea con la finalidad de regular la función financiera contable y de auditoría de las empresas registradas en las bolsa de valores *New York Stock Exchange* (NYSE) y/o en la *National Association of Securities Dealers by Automatic Quotation* (NASDAQ).

Las empresas mexicanas enlistadas con ADRs (Programas de *American Depositary Receipts*) en la bolsa de valores de Estados Unidos son: Televisa (Televisora), América Móvil (telefonía móvil), Coca-Cola y Cerveza Sol FEMSA (embotelladora), FEMSA Comercio (Oxxo), Empresa ICA (construcción), Grupos Aeroportuarios Norte, Pacífico y Sureste, Casa Saba (medicamentos), Industrias Bachoco (venta de pollo y huevo), Maxcom Telecomunicaciones, Vitro (productor de vidrio, Cemex (productor de cemento), Gruma (productor de maíz y tortilla), Grupo Radio Centro (Radiofónica), y TELMEX (telefonía fija).

Es una legislación que penaliza fraudes, corrupción administrativa, conflictos de intereses y negligencia profesional o ejecutiva; que afectan a los socios, empleados, clientes y proveedores. Se compone de seis áreas, todas están enfocadas a situaciones diferentes pero con el mismo objetivo, el cual consiste en ofrecer una mejora continua al proceso actual; la primera se encarga de la calidad en la información pública, la segunda de buenas prácticas en un gobierno corporativo, la tercera en las conductas y comportamientos, la cuarta en las actuaciones en los mercados cotizados, la quinta en las sanciones a incumplimientos, y la última en la independencia efectiva de los auditores.

Por su contenido extenso, a continuación se describen las secciones que resultan de interés al tema abordado, retomando a Danilo (2002):

Sección II-206. *Conflictos de Interés y responsabilidades de los órganos de control y supervisión.*

Cuando las malas prácticas destruyen la armonía corporativa, se pierde la confianza en las operaciones, gestión e informes de la misma; una forma de crear un ambiente equilibrado es analizar el desempeño de las operaciones en base a los siguientes aspectos:

- **Organigrama**; es una gráfica que debe presentar además de la estructura organizacional, líneas de comunicación fiables para la asignación de obligaciones y cumplimiento de responsabilidades, entre los diferentes departamentos u oficinas.
- **Políticas y reglamentos**; la definición de funciones, la asignación de responsable y la regulación de conductas son acciones que deben estar por escritos en manuales de actividades, descripción de puestos y manuales de procedimientos, que brinde información necesaria para contestar las siguientes interrogantes: ¿Qué se va hacer?, ¿Quién lo va a realizar?, ¿Cómo se hará?, asimismo, debe contemplar alternativas definidas imparcialmente ante posibles casos esperados pero no deseados.
- **Misión, Visión, Metas y Estrategias**; el éxito no se logra solamente con el hecho de difundir el conocimiento, se obtiene cuando cada integrante "se pone la camiseta" comprometido porque está convencido de la importancia que tiene su presencia en el contexto global.
- **Riesgos.** Cuántas veces se escuchan refranes populares como: "a niño ahogado; pozo tapado" o "más vale prevenir; que lamentar", ambos hacen referencia a la falta de una conducta en prevención; en donde los siniestros son las principales consecuencias de malas decisiones o acciones. Una forma de abatir este problema es contar con un análisis de riesgos elaborado en forma conjunta por un administrador, contador y auditor, en el cual se contemplen las amenazas, la probabilidad de ocurrencia, las acciones preventivas, correctivas, el costo y tiempo de recuperación, en el caso de que sucedan.
- **Reportes**. Deben presentar información confiable, oportuna y segura.
- **Tecnología**. Se relaciona con los términos de *software, hardware*, equipo de comunicación e infraestructura, que juntos se han convertido en la principal herramienta de apoyo para dar soporte y protección a las transacciones presenciales y/o en línea; pero, cabe hacer mención que el mejor equipo no garantiza estar exento a fraudes y una forma de medir la vulnerabilidad es aplicar pruebas de penetración al mismo sistema.

Sección 404. *Evaluación Gerencial de los Controles Internos*

La certificación del control interno financiero y la seguridad de las tecnologías en información son conceptos que se relacionan al momento de emplear equipos de cómputo y de comunicaciones para los controles de acceso, de cambios, de monitoreo y supervisión de las transacciones financieras y contables que realizan el Director y el auditor de cuentas, con el objetivo de evaluar que los estados financieros no estén alterados de manera accidental o premeditada. Para verificar el buen funcionamiento de la organización, debe revisarse la existencia y aplicación de los siguientes documentos sobre el control y uso de la tecnología:

- Políticas y reglamentos sobre el uso y control de infraestructura, equipo y personal relacionados a las actividades financieras.
- Manual de procedimientos y procesos para el desarrollo de informes financieros.
- Manual de funciones de gestores de los sistemas de información financiera (incluye gestores de bases de datos).
- Informes financieros, realizado por los gestores de sistemas y avalados por auditores externos expertos en finanzas y en sistemas.
- Código de ética de los gestores de sistemas que regule los intereses personales y profesionales.

La Tecnología en un marco legal

Actualmente las tecnologías son una herramienta fundamental para el quehacer operativo, financiero y contable de una organización; y una forma de evaluar la efectividad de sus controles de acceso, altas, bajas y modificaciones de datos, recertificaciones, segregación de funciones, control de cambios a producción de infraestructura tecnológica y sistemas, monitoreo de accesos privilegiados, políticas y estándares, manejo de incidentes y problemas, y otras; es cumplir con la ley SOX; sin embargo, es necesario apoyarse en metodologías reconocidas mundialmente como: *International Standard Organization* (ISO) y *Control Objectives for Information and related Technology* (COBIT), debido a que la legislación no indica literalmente lo que se debe de revisar, (Alberto, 2011).

2.3.2. Ley *Stop Online Piracy Acy* (SOPA)

Por sus siglas en Ingles se denomina *Stop Online Piracy Act*, es una regulación propuesta por empresas y organizaciones americanas en espera de regular la piratería en el diseño, contenido y empleo de páginas *web*. Actualmente está en espera de ser aprobada por el Congreso de los Estados Unidos y en caso de ser así muchos sitios que ofrecen servicios de investigación, recreación y otros más, se cerrarían al comprobar que violan los derechos de autor o de la propiedad intelectual. Esta ley fue creada para traspasar fronteras, porque la mayoría de los sitios depende de la infraestructura norteamericana y debe sujetarse a su legislación.

El *internet* cambiará de estructura, se implementarán nuevas regulaciones a los medios de distribución de documentos, películas, música y programas que quieran formar parte de esta red; empresas como *Wikipedia, Google* y *Youtube* tendrán que ajustarse al nuevo modelo o se quedaran sin contenidos; asimismo, afectará a usuarios particulares que utilicen correos electrónicos, redes sociales y *blogs* con imágenes, videos, textos y referencias de hipertexto que no tengan la aprobación del autor o sean denunciados por los mismos. Los servidores tendrán una nueva misión: "Que todos los contenidos que se filtren en *internet* sean transparentes y aprobados legalmente"; de lo contrario la acción "bloquear" pasará de ser un riesgo a una amenaza, en los siguientes casos:

a) Foro bloqueado por no filtrar el contenido subido por sus participantes.
b) Blog bloqueado por aceptar enlaces a un "sitio denunciado" de alojamiento ilegal de contenido con *copyright*
c) Sitio bloqueado por reproducir obras como canciones, poemas, videos, imágenes con *copyright.*

En el caso a) y b) existe un plazo de cinco días naturales para ser exonerados, siempre y cuando, se realicen las siguientes acciones:

- Bloquear el acceso al dominio responsable
- Bloquear el acceso al sitio
- Bloquear la publicidad
- Bloquear el pago al servicio
- Bloquear enlaces a otro sitio

Aunque muchos usuarios cuestionen el grado de coacción que tiene la protección de la propiedad intelectual sobre la libertad de expresión en *internet,* es responsabilidad del auditor comprobar que los sitios se encuentran trabajando dentro del marco legal; (Remixado, 2012).

CAPÍTULO III

PROGRAMAS DIAGNÓSTICOS DE AUDITORÍA INFORMÁTICA

WinAudit, OpenAudit, FreshDiagnose, Lansweeper, Total Networks Inventory, SoftKey, Taw, WhatWeb, XRumer, Watobo, Secure Auditor, ApexSQL, Nessus, NMAP, WhireShark

3.1. La Tecnología auditando a la Tecnología

Cuando se piensa en realizar una Auditoría en Informática, vienen a la mente varios aspectos a evaluar dentro de un computador; esta actividad sería muy laboriosa si en la actualidad no existieran programas de diagnóstico que apoyan esta función, generando reportes en las categorías de *software, hardware*, dispositivos, base de datos, redes e *internet.* Son muy eficientes y pueden presentar un inventario en segundos por equipo, con la relación del *software* instalado, del sistema de arranque y la licencias de los mismos; así también, ofrecen un informe detallado con las características del microprocesador, memoria, discos lógicos, unidades extraíbles, puertos de comunicación, protocolos de red y direcciones IP, entre otras, el cual puede ser emitido en formato de texto, PDF, HTML, o exportado a una base de datos.

Para un auditor son considerados como herramientas de trabajo que facilitan el diagnóstico de cada equipo, y la experiencia con los conocimientos del profesional juegan un papel muy importante para la interpretación adecuada de las características de *hardware, software* y servicios, contenida en los reportes; ahora el único dilema será seleccionar la opción más adecuada según las características de los computadores a auditar, entre las cuales puede mencionarse: al sistema operativo, número de máquinas, conexión de red e incluso metodología de trabajo. A continuación se presentan algunos de ellos, con la finalidad de conocer los servicios que ofrece cada uno *(ver Fig. 21).*

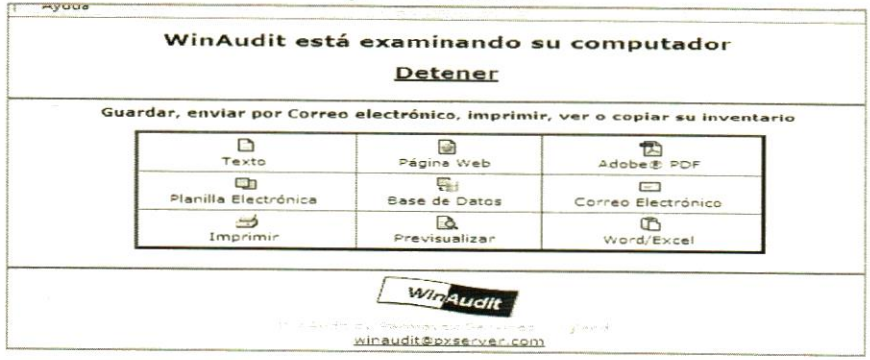
Figura 21. Programas de Diagnóstico

Fuente: [elaboración propia con Logotipos existentes en *internet]*

3.2. WinAudit

Es un programa gratuito al alcance de todos, con interfaces sencillas que en pocos segundos y tras del análisis de un computador presenta un informe completo de sus programas instalados, sistema operativo, procesador, memoria y discos duros que contenga. Esta información puede ser emitida o impresa en un archivo de texto, PDF, CSV, HTML o XML; con base a (WinAudit).

Figura 22. WinAudit



Fuente: [Pantallas del Programa]

Se describe algunas pasos que se ejecutan en el análisis:

1. Inicia el análisis de la información, el tiempo varía en cada computador en relación a la cantidad de *software* y controladores instalados.
2. Presenta nueve formatos para la impresión del informe: Texto, Página *Web*, PDF, Planilla electrónica, Base de Datos, Correo Electrónico, *Word* y *Excel, (ver Fig. 22).*
3. La opción de Vista General presenta el nombre de la PC, dominio, sitio, roles, descripción, sistema operativo, compañía manufacturera, modelo y número de serie del equipo, número y descripción de procesador, total de memoria, total del disco duro, pantalla, versión de la BIOS, cuenta del usuario y hora del sistema.
4. La opción de *software* instalado presenta las siguientes características de todos los programas instalados: nombre, proveedor, versión, idioma, dato, locación, fuente y estado de instalación, tipo, código y nombre de paquete, id producto, registro de compañía y del cliente, ruta, versión y descripción ejecutable, id *software*, entre otros. Generalmente no se obtiene la información completa de cada *software*.

5. La selección de categorías a inventariar contiene: las siguientes opciones para que el usuario elija libremente: Sistema Operativo, Periféricos, Seguridad, Grupos y Usuarios, Tareas Programadas, Red *Windows*, Red TCP/IP, NetBIOS, Dispositivos, Procesadores, Memoria, Discos Físicos, Disco Lógicos, Puertos de Comunicación, Programas de Arranque, Servicios, Programas en ejecución y otros, *(ver Fig. 23)*.

6. Al finalizar se emite un reporte diagnóstico el cual se puede guardar, imprimir o enviar por correo electrónico.

Figura 23, WinAudit [categorías]

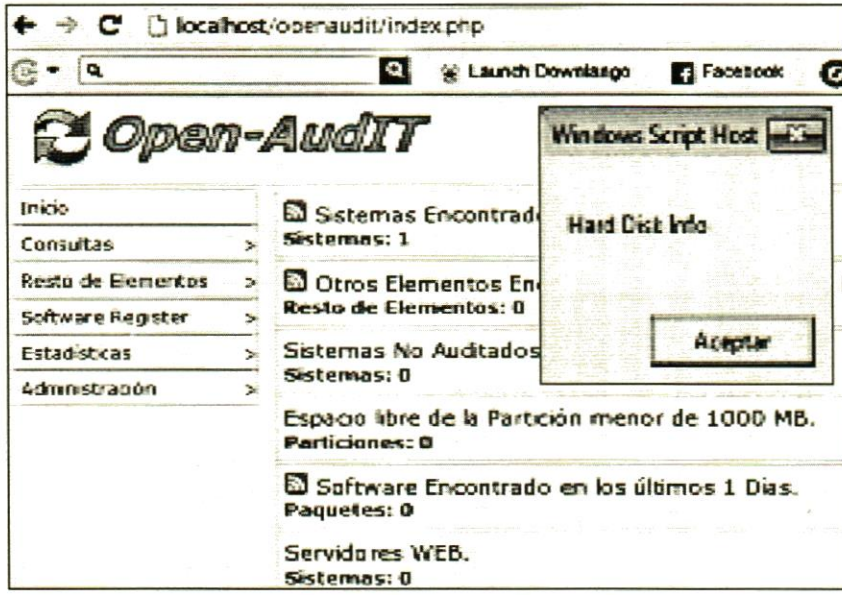
Fuente: [Pantallas del Programa]

3.3. OpenAudit

Es un programa de aplicación que trabaja en la plataforma *Windows* y *Linux;* con la capacidad de ser configurado para diagnosticar a través de la red los equipos conectados. Presenta información respecto al *hardware*, *software*, configuración del sistema operativo, configuraciones de seguridad, servicios de usuarios y servicios de comunicación (*switches, routers*, etc); entre otros, por medio de reportes en formato *Web*, PDF y CVS.

Entre los requisitos de instalación se encuentra el Apache, MySQL y PHP. Con base a información de *OpenAudit.*

Figura 24. OpenAudit



Fuente: [Pantallas del Programa].

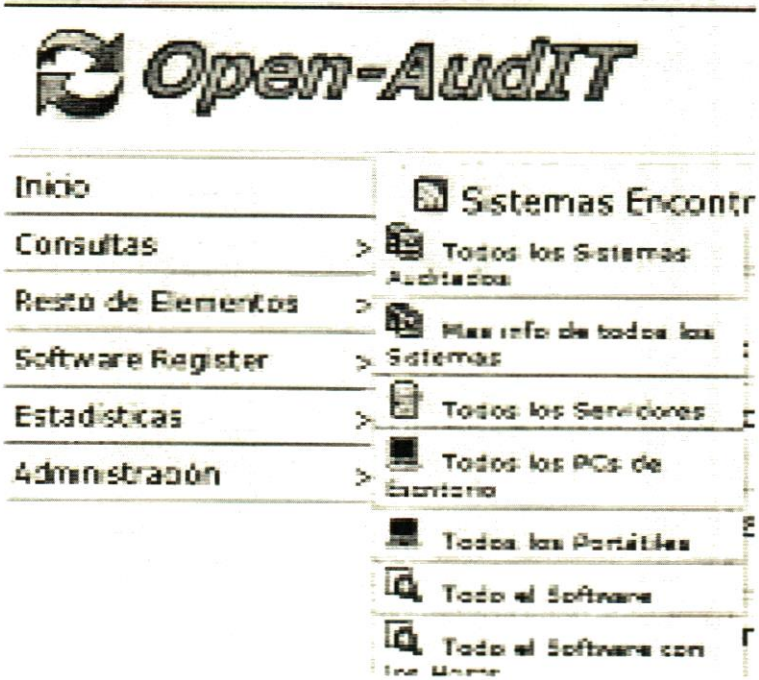
Se describen puntos que se ejecutan en el análisis:

1. En la pantalla Principal se presenta el número de Sistemas y Elementos encontrados en los últimos 3 días, Sistemas no auditados, Espacio libre de la partición menos de 1000 MB, Servidores WEB, FTP, *Telnet* y otros. (*Ver Fig. 24).*
2. Gradualmente se presentan los componentes a revisar: de impresora, disco duro, partición, tarjeta SCSI, unidad óptica, mouse, tarjeta de sonido, red, etc. (*Ver Fig. 24).*
3. La información puede presentarse por medio de los siguientes módulos y sub módulos correspondientes:
    - Consultas: Sistemas auditados, Servidores, Portátiles, Computadoras de Escritorio, *software* y más. (*Ver Fig.25).*
    - Otros Elementos: Impresoras, Monitores, Red, Dispositivos.
    - *Software* Registrado: Agregar y borrar software, espacio libre de la partición.

- Estadísticas: Tipo SO, versión IT, versión explorador, tamaño de memoria, tipo procesador, disco duro, claves, *Gateway*.

4. Los reportes son en página *Web* y en *Excel*.

Figura 25. OpenAudit [Módulos]



Fuente: [Pantallas del Programa].

3.4. Fresh Diagnose

Es un programa fácil de manejar que permite analizar rápidamente a un computador y generar un reporte de las siguientes áreas: Sistema de *software*, Sistema del *hardware*, Dispositivos, Red e *Internet,* Multimedia, Sistema de Bases de Datos, Recursos de *hardware*, Foto, Rastros, Pruebas Patrones. Asimismo, brinda información específica de cada una, (Fresh Diagnose).

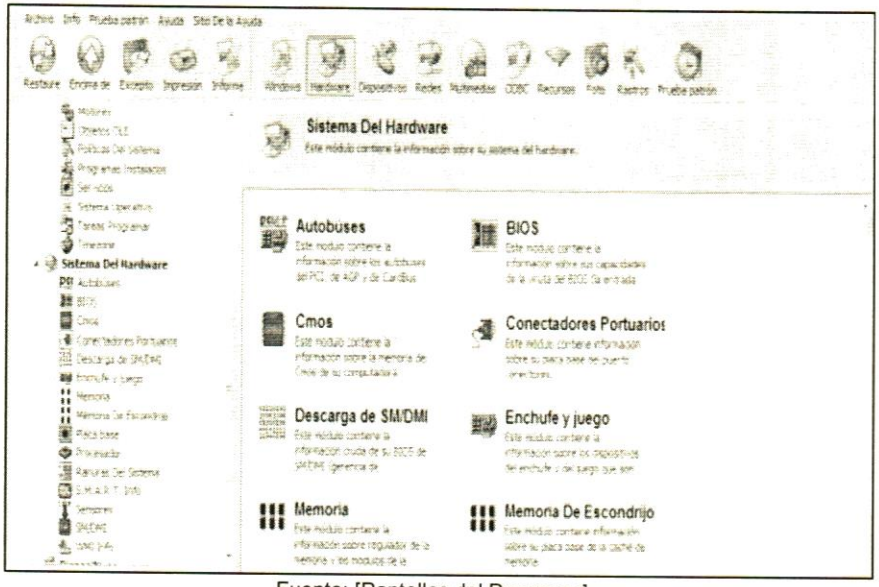
Figura 26 . Fresh Diagnose [Software]

Fuente: [Pantallas del Programa]

Se describen los componentes de cada módulo que intervienen en el análisis:

1. El Sistema de *Software* contiene: Accesibilidad, Actualizaciones de *Windows*, Ajustes Regionales, Ambiente, Arranque, Asociaciones del Archivo, Aspecto, Carpetas de la Cáscara, Certificados, Consola del Comando. *(ver Fig.26)*.
2. Red e *Internet* contiene: Red, adaptadores de Red, Configuración de TCP/IP, Configuración de *NetBios, Winsock*, Ajustes del *Internet*, *Internet Explorer*, Zonas del *Internet, Browser* Ayudante y Cuentas del Correo.
3. Multimedia contiene: *DirectX, DirectDraw, DirectSound*, Auxiliar, Palanca de mando, Control de los Medios, Mezclador, Midi Adentro, Midi hacia afuera, Onda Adentro.
4. Sistema de *hardware* contiene: Autobuses, BIOS, Cmos, Conectadores Portuarios, Descarga de SM/DMI, Enchufe y juego, Memoria, Memoria de Escondrijo, Placa base, Procesador. *(Ver Fig.27)*.
5. Dispositivos contiene: *Harddisks,* Monitores de Exhibición, Particiones, Teclado, Puertos, *Optical Drivers*, Adaptadores de Exhibición, lógica *Drivers*, Ratón, Impresoras.

Figura 27. Fresh Diagnose [Hardware]



Fuente: [Pantallas del Programa]

6. Foto: Procesos, *Modules*, Hilos de roscas, Montones, *Windows*, Archivos Compartidos.
7. Prueba de patrones: Procesador *Benchmark,* Adaptador de Video, CD *Benchmark,* Prueba patrón de multimedia, video, memorias, disco duro y de la red.
8. Sistema de la Base de Datos; base de ODBC, conductores de ODBC, Convertidores de ODBC, Fuentes de Datos de OD.
9. Recursos de *hardware*: Peticiones de la Interrupción, Canales de Acceso Directo, puertos E/S, recursos de la memoria.
10. Rastros: Archivos Ejecutados, Historia de *Windows*, Historia de la Búsqueda, Funcione La Historia, *Openand* Ahorra Historia, Historia del *Browser*, Archivos Recientes, Escondrijo del *Internet*, Galletas del *Internet*, Dispositivos.

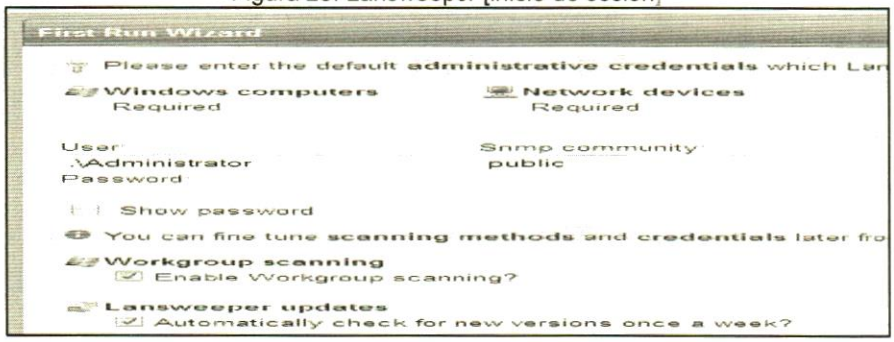
Los Reportes se presentan en HTML y ofrece las opciones de:

a) Sistema de SW/ Accesibilidad
b) Sistema de HW/ Memoria

3.5. Lansweeper

Es un programa que permite realizar el inventario de los equipos que se encuentran conectados en una red, entre las principales características presenta información de usuario, *hardware, software* (parches y licencias), configuración del equipo, configuración del *Windows*, procesos de ejecución y registro de entradas, que es almacenada en un servidor SQL Los reportes son exportados en formatos XLS, CVS y XML.

Figura 28. Lansweeper [inicio de sesión]

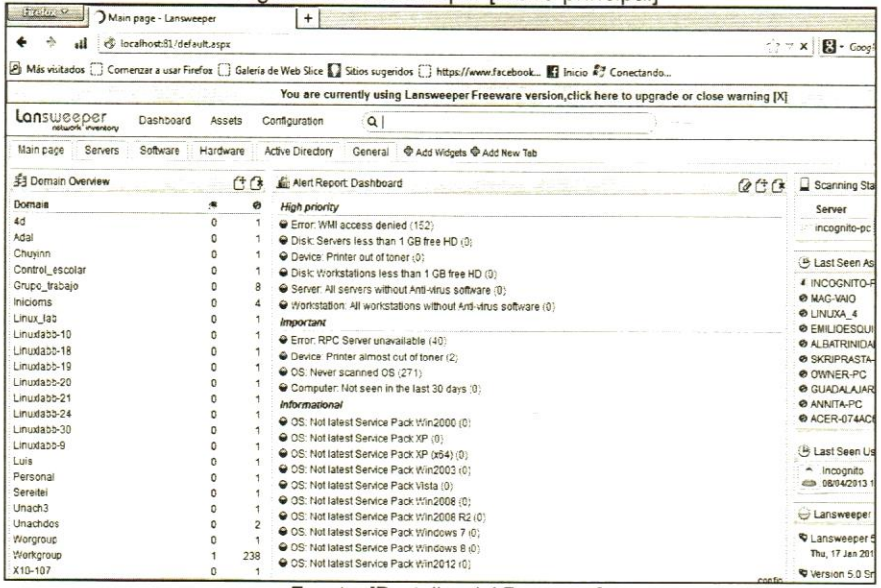


Fuente: [Pantallas del Programa]

Se describen algunos puntos que se ejecutan en el análisis:

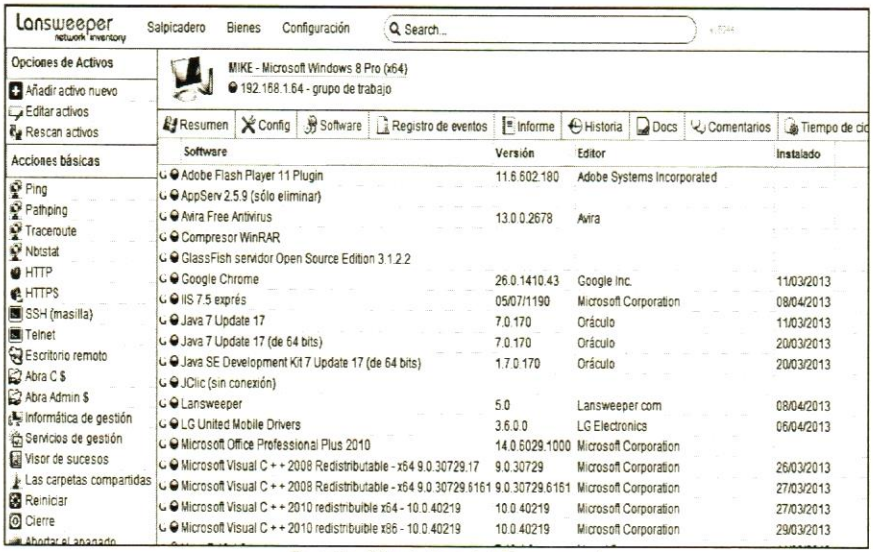
1. Se inicia con el nombre de usuario y el contraseña correspondiente, asimismo, se especifica las características del grupo de trabajo y el rango de IP. *(Ver Fig. 28).*
2. El Menú Principal Presenta el nombre de cada equipo conectado en la red que los identifica como Dominios, un reporte de alertas clasificados por prioridades, una lista de usuarios y un historial. *(Ver Fig.29)*
3. El Módulo de *software* presenta Información de los programas instalados y el reporte de alerta de *software*.
4. El Módulo de *hardware* indica características, capacidad de los componentes, reporte de alerta de *hardware* y de dispositivos.
5. Los reportes se presentan en página *Web* y en hoja de Cálculo *Excel*, contienen nombre del *software*, versión, proveedor y fecha de instalación. *(Ver Fig. 30).*
6. El programa también incluye las opciones de página principal, Servidores y Directorio.

Figura 29. Lansweeper [menú principal]



Fuente: [Pantallas del Programa]

Figura 30. Lansweeper [impresión}



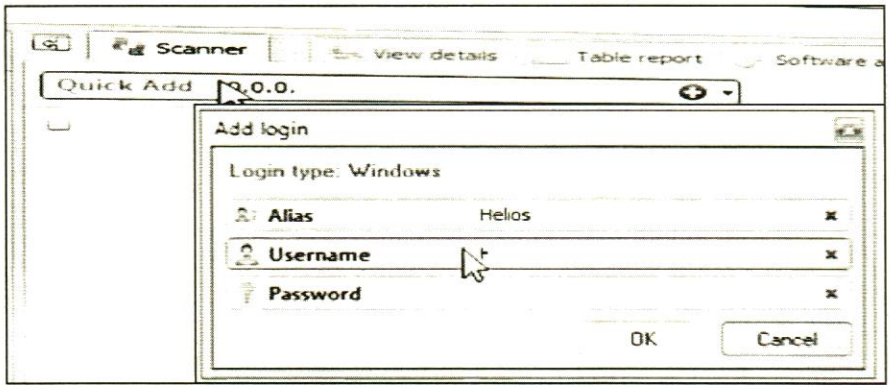
Fuente: [Pantallas del Programa]

3.6. *Total Networks Inventory*

Es un programa que ofrece un inventario del *software* y hardware de los equipos conectados a una red. Trabaja sobre la plataforma de *Windows*, *Mac OS* y *Linux*. Ofrece una prueba de 60 días con instalación fácil y práctica lista para usarse, solo es necesario introducir la contraseña del administrador.

Entre otros servicios ofrece la creación de una base de datos de los usuarios de la red y el seguimiento en línea de los equipos en tiempo real, (Total Network Inventory).

Figura 31. Total Networks Inventory

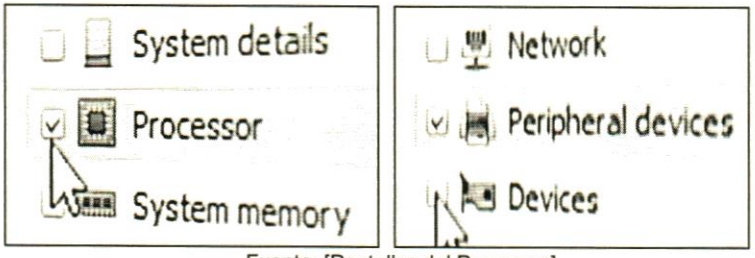


Fuente: [Pantallas del Programa]

Se describen algunos puntos del proceso de análisis:

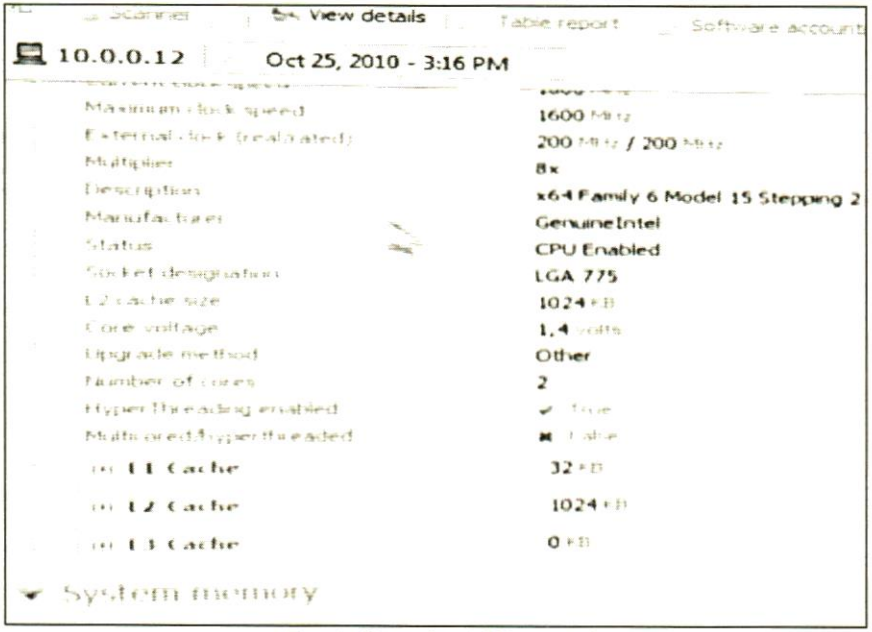
1. Para realizar un monitoreo a la red; es necesario teclear el nombre de usuario y contraseña. Asimismo definir el rango de direcciones IP o seleccionar un equipo específico *(ver Fig.31)*
2. Se realiza el inventario exhaustivo de cada equipo, sin importar la plataforma de Sistema Operativo,
3. Permite seleccionar algunos de los puntos que se escanean en uno o varios equipos al mismo tiempo, en relación al *hardware, software*, usuarios y seguridad, que pueden ser detalles del sistema, procesador, sistema de memoria, redes, dispositivos, recursos compartidos y servicios, entre otros. *(Ver Fig.32)*
4. En el diagnóstico del equipo se encuentra información en relación al tamaño de la memoria *cache* (nivel 1, nivel 2 y nivel 3), reloj externo, memoria física, memoria virtual, *slots* de memorias, memoria de video *Ram*, capacidad de los Disco Duros instalados, y mucho más *(ver Fig. 33)*.

Figura 32. Total Networks Inventory [escaneo]



Fuente: [Pantallas del Programa]

Figura 33. Total Networks Inventory [diagnóstico]



Fuente: [Pantallas del Programa]

5. Después del Diagnóstico se presenta el Informe con la opción de imprimir o guardar.
6. *Total Network Inventory* también presenta la información de la direcciones MAC a partir de su dirección IP en forma tabular.

Además, incluye las opciones de escaneo, reporte y *software*.

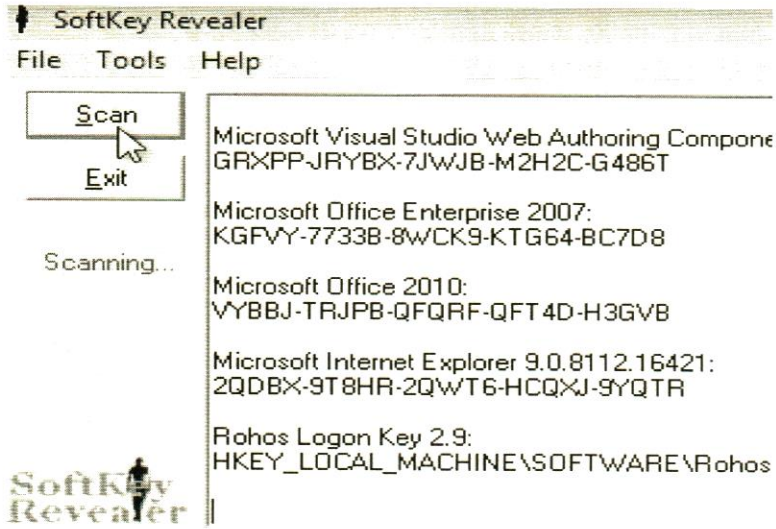
3.7. Softkey

Es un programa con una interfaz simple y sencilla, fácil de entender y manejar; que revisa el ordenador y presenta exclusivamente la lista de los programas que tienen licencia o número de serie en un formato de texto. Con base a (Softkey).

Se describe los puntos del proceso de análisis *(Ver Fig. 34):*

1. El menú Archivo incluye las opciones de: Grabar, Copiar a *Word*, Imprimir o Salir.
2. El menú Herramientas incluye las opciones de: Descifrar claves *Adobe*, contraseñas eliminadas, claves modificadas, información de *Windows*.
3. El menú Ayuda incluye las opciones de: página principal y acerca de
4. El botón escanea: realiza el análisis del equipo, presentando el nombre y la licencia del *software* instalado.
5. El botón de salida: termina el programa.
6. El reporte se genera en el editor de texto de *Word.*

Figura 34. Softkey

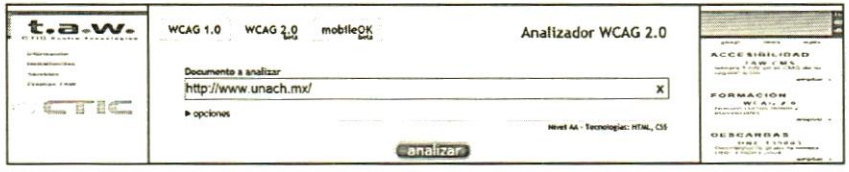


Fuente: [Pantallas del Programa]

3.8. TAW (Test de Accesibilidad Web)

Es una aplicación de interfaz múltiple que revisa en tiempo real la accesibilidad del contenido de una página o de un sitio completo, esta metodología facilita un análisis simultáneo de varios aspectos de la página o de diferentes sitios *WEB*, con solo registra la *URL* se presenta un informe en HTML con las incidencias encontradas, en base a (TAW).

Figura 35. TAW

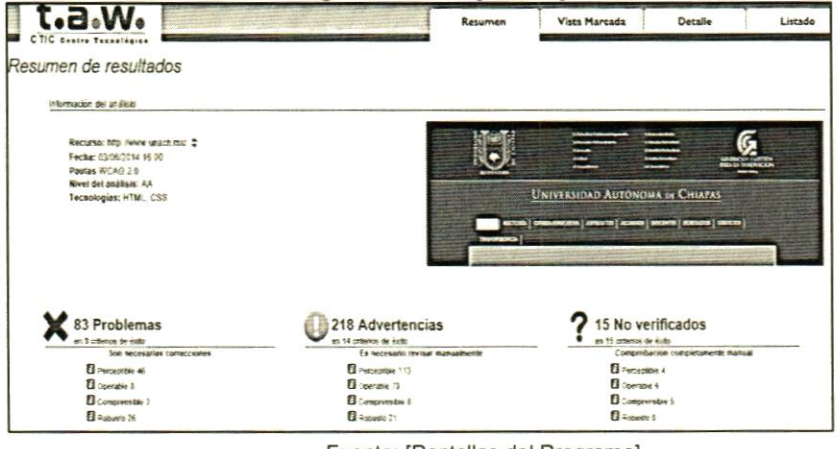


Fuente: [Pantallas del Programa]

Puntos del proceso de análisis:

1. Se ingresa la URL o página para ser analizada. *(Ver Fig.35).*
2. En el resumen de resultados, se aprecia el recurso, la fecha y las pautas de evaluación, el nivel de análisis y la tecnología empleada. Asimismo incluye la notificación de Problemas, Advertencias y los No verificados. *(Ver Fig.36).*
3. En el Resultado de análisis las incidencias se clasifican por principio "perceptible, operable, comprensible y robusto", y por tecnología.

Figura 36. TAW [viñetas]



Fuente: [Pantallas del Programa]

Para diseñar la página, hay que cumplir con las Pautas de Accesibilidad para el Contenido *Web*, al cumplirlas permite incrementar el número visitantes, incluyendo a las personas que tengan alguna capacidad diferente relacionada a la deficiencia de audio, visión, lenguaje, cognitivas, entre otras, en base a (W3C, 2009). Las pautas se clasifican en principios:

- *Principio 1. Perceptible*

1.1. Alternativa textual. Se refiere a textos ampliados, *braille*, voz, símbolos o lenguaje simple.
1.2. Tempo dependiente. Proporcionar alternativas para los medios de audio y video grabado.
1.3. Adaptable. Contenido que pueda presentarse de diferentes formas.
1.4. Distinguible. Facilidad para ver y oír el contenido. Incluyendo la separación entre el primer plano y el fondo.

- *Principio 2.Operable*

2.1. Accesible por teclado
2.2. Tiempo suficiente para leer y usar el contenido.
2.3. Convulsiones. Una página no debe contener nada que destelle más de tres veces por segundo.
2.4. Navegable. Titular páginas, encabezados, etiquetas, propósito de los enlaces, proporcionar múltiples vías.

- *Principio 3. Comprensibles*

3.1. Legible y comprensible los contenidos. Idioma, palabras inusuales, abreviaturas, pronunciación.
3.2. Predecibles. Coherencia en las páginas al momento de la navegación.
3.3. Entrada de datos asistida para evitar y corregir errores de los usuarios.

- *Principio 4. Robusto*

4.1. Compatible con las aplicaciones actuales y futuras.

De acuerdo con Díaz, Harari y Amadeo (2007), entre los errores más comunes se encuentran:

- Falta de información relevante en el *Header* de HTML, por ejemplo el idioma, la versión y la codificación ISO usada en el documento
- Falta de texto alternativos en las imágenes, íconos e hipervínculos
- En las hojas de estilo, usar medidas relativas
- No utilizar el *&accute* para los acentos y códigos ñ
- Falta de información de resumen en las tablas
- Falta de títulos en los *frames* utilizados

3.9. WhatWeb

Aplicación que mide principalmente la seguridad de servidores, trabaja en modo consola en sistemas *Linux* y ofrece más de un millón de *plugins* para facilitar su configuración. Tiene la capacidad de reconocer tecnologías *Web*, incluyendo los sistemas de gestión de contenidos (CMS), plataformas de *blogs*, paquetes estadísticos, bibliotecas de *JavaScript*, servidores *web* y dispositivos embebidos. Además puede identificar números de versión, direcciones de correos electrónicos, identificadores cuenta, módulos de *framework web* y errores de SQL. Un sitio *Web* se vuelve vulnerable con los rastros que otorga en la visita de una página, puede haber dos tipos de agresiones, la pasiva solo requiere la solicitud HTTP y la agresiva incluye pruebas de penetración; en base a (WhatWeb, 2011).

Aplicando *WhatWeb* se puede realizar un análisis detallado de un sitio *web (ver Fig. 37),* conocer el servidor y el protocolo que emplea, la dirección IP, el lugar de origen e información de la página solicitada.

Figura 37. WhatWeb

```
$ ./whatweb -v www.morningstarsecurity.com
www.morningstarsecurity.com/ [200]
http://www.morningstarsecurity.com [200] Google-Talk-Chatback, WordPress[3.1], F
oogle-API[ajax/libs/jquery/1.3.2/jquery.min.js], Script, MetaGenerator[WordPress
HTTPServer[Apache], x-pingback[,http://www.morningstarsecurity.com/xmlrpc.php],
Analytics[GA][791888], UncommonHeaders[x-pingback], Apache, IP[210.48.71.202], J
.4.4], Title[MorningStar Security], Country[NEW ZEALAND][NZ]
URL     : http://www.morningstarsecurity.com
Status  : 200
   Apache ----------------------------------------------------------------
        Description: The Apache HTTP Server Project is an effort to develop and
                     maintain an open-source HTTP server for modern operating
                     systems including UNIX and Windows NT. The goal of this
                     project is to provide a secure, efficient and extensible
                     server that provides HTTP services in sync with the current
                     HTTP standards. - homepage: http://httpd.apache.org/
        Certainty  : certain

   Country ---------------------------------------------------------------
        Description: GeoIP IP2Country lookup. To refresh DB, replace
                     IpToCountry.csv and remove country-ips.dat. GeoIP database
                     from http://software77.net/geo-ip/. Local IPv4 addresses
                     are represented as ZZ according to an ISO convention.
                     Lookup code developed by Matthias Wachter for rubyquiz.com
                     and used with permission.
        Certainty  : certain
        Module     : NZ
        String     : NEW ZEALAND

   Title -----------------------------------------------------------------
        Description: The HTML page title
        Certainty  : certain
        String     : MorningStar Security (from page title)
```

Fuente: [Pantallas del Programa]

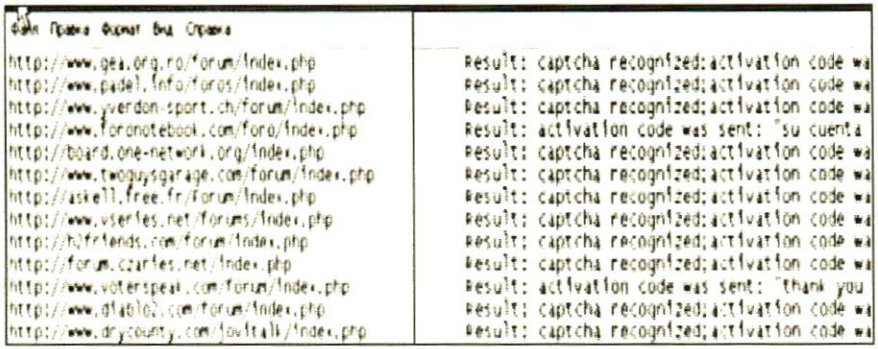
3.10. XRumer

Es una herramienta de publicación que puede enviar mensajes privados a los usuarios de los foros, mensajes para todos los tipos de *blogs*, libros de visitas, galerías de imágenes, directorios de enlaces que tienen diferentes tipos de cifrado; es por eso que para fines de auditoría se puede emplear como prueba de penetración para evaluar la seguridad de los sitios desarrollados con *phpBB, phpNuke, yaBB, VBulletin, Invision Power Board, IconBoard, UltimateBB,exBB y phorum.org*. Su función consiste en registrarse como usuario y enviar *spam* y *links* a sitios *web, blogs* o foros, que han sido infectados con *malware*; y probar el nivel de resistencia para proteger el cifrado captcha, y el bloqueo de direcciones IP sospechosas; en base a (XRumer, 2013).

Se describen puntos del proceso de análisis:

1. Se realiza el registro del usuario con el ID, página, correo y otros datos, Asimismo, se escribe el mensaje de texto que aparecerá en otras páginas y se marca la prioridad de las categorías, por ejemplo: "*SEO, Doorway, black hat, spam, Bood*".
2. La ejecución de *XRumer* consiste en conectarse a varios sitios, foros y correos, descifrando los códigos e incluyendo los encriptados "captcha". *(Ver Fig.38)*.
3. El acceso es en forma remota a las páginas más vulnerables y deposita en su bandeja el mensaje elaborado sin la autorización del propietario o administrador del sitio.

Figura 38. XRumer



Fuente: [Pantallas del Programa]

3.11. Watobo

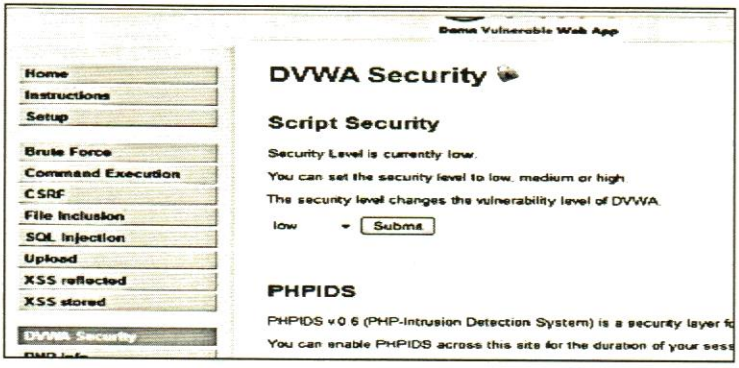
Es un programa de *software* libre, que trabaja en las plataformas de Linux, Windows y *Mac.* Su principal ventaja para evaluar la seguridad de las aplicaciones *Web* es actuar como si fuera un *proxy* local. Está compuesto de controles pasivos y activos, los primeros permiten extraer información sobre direcciones IP y de correos electrónicos; y los segundos emiten peticiones como inyecciones de SQL para detectar las vulnerabilidades. Las características más importantes son: gestión de sesiones, funciones de filtro inteligente, escáner de vulnerabilidades, *fuzzer*, etc., en base a (Watobo, 2011).

Para instalarlo se descarga *Ruby y DevKit* de la página http://rubyinstaller.org/downloads, *DevKit* se aloja en raíz y se inicializa (dk.rb init) e instala (dk.rb install y gem install watobo) desde línea de comando. Al finalizar los procesos con éxito, se teclea *watobo_gui* para ejecutarlo.

Se describen puntos del proceso de análisis:

1. Se crea un proyecto y se inicia una sesión
2. Se ingresa con la cuenta de administrador al sitio DVWA para identificar las funciones más importantes sobre nivel de seguridad clasificadas en bajo, medio y alto; y protección PHPPIDS, también incluye los botones: "Inicio, instrucciones, configuración, fuerza bruta, comando de ejecución, CSRF, archivos de inclusión, inyección SQL". *(Ver fig. 39).*

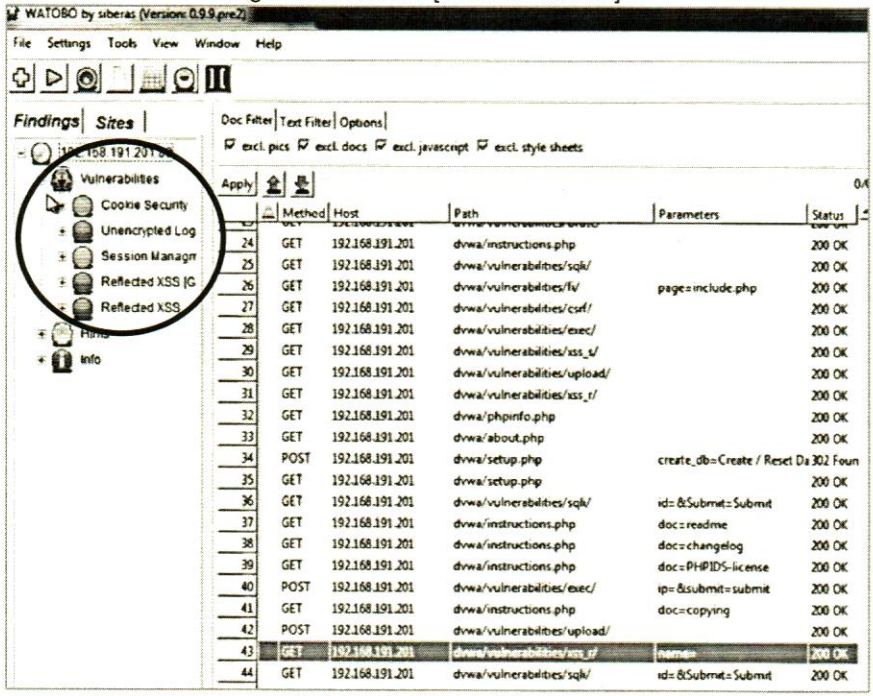
Figura 39. Watobo [seguridad]



Fuente: [Pantallas del Programa]

3. Al terminar la configuración se presenta una tabla de conversación con más peticiones para examinar y un listado de vulnerabilidades, entre ellas se presentan: *"Cookie Security, Unencrypted ,Session Managment"*. Asimismo incluye una ventana que indica el método, la dirección IP, ruta, parámetros y estado. *(Ver Fig. 40)*; en base a (Watobo, 2012).

Figura 40. Watobo [vulnerabilidades]



Fuente: [Pantallas del Programa

3.12. Secure SQL Auditor

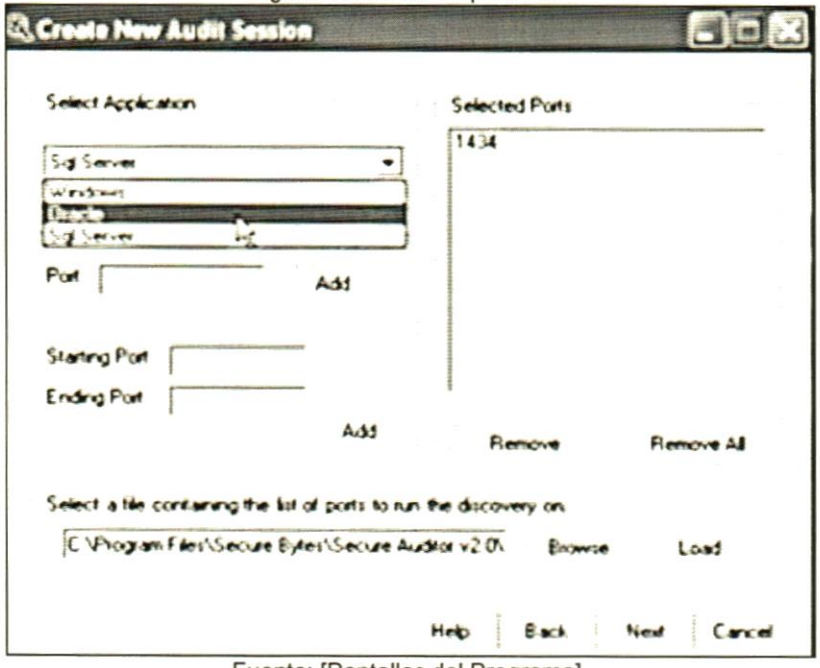
Es un programa que se especializa en la seguridad de redes y base de datos. En redes ofrece mayor protección para los cortafuegos PIX Y ASA, conmutadores y enrutadores Cisco. Asimismo, puede controlar contraseñas, controles de accesos, configuraciones erróneas, mecanismos de autenticación, vulnerabilidades basadas en HTTP y en IOS; en base a (*Secure Auditor*).

En base de datos puede mencionarse que ***Secure SQL Auditor***, detecta las vulnerabilidades y amenazas de los servidores de base de datos SQL, y gracias a su diseño en ambiente de red puede escanear múltiples servidores, al finalizar el análisis presenta un informe con las soluciones propuestas de los problemas detectados, entre los más comunes están los derechos de acceso, política de contraseñas, roles de bases de datos e integridad de sistema; en base a (*SecureSqlAuditor*).

Se describen puntos del proceso de análisis:

1. Se crea una sesión asignando un rango de direcciones IP y el tipo de escaneo.
2. Se define la aplicación, que puede ser: *Windows*, Cisco, *Oracle* o *SqlServer*; también se indica el puerto. *(Ver Fig. 41)*.
3. Cuando finaliza el diagnóstico, nos presenta la información general y vulnerabilidades de todos y cada uno de los equipos conectados a la red, organizados por sistemas operativos.

Figura 41. Secure Sql Auditor



Fuente: [Pantallas del Programa]

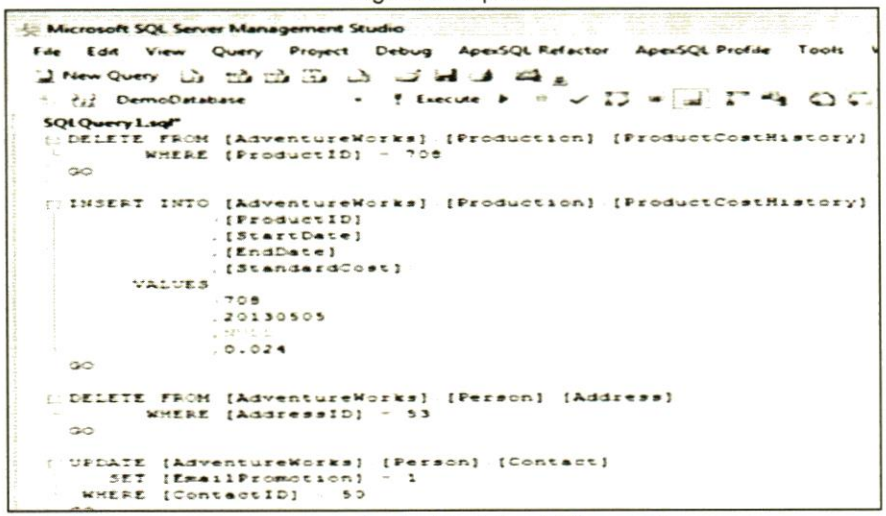
3.13. ApexSQL

Es un programa de aplicación de *Microsoft,* que ofrece la oportunidad de explorar el registro de transacciones para ver quien los creó, los detalles de un accidente, los cambios de permisos, revertir los cambios de la base de datos, recuperar datos perdidos o dañados, identificar usuarios, permisos de seguimiento de cambios, aislar operaciones por fecha y objeto, y/o crear informes; en base a (Apex SQL, 2014).

Se describen puntos del proceso de análisis:

1. Seleccionar las tablas con las que se van a trabajar en la base de datos y asignar los atributos "insertar, actualizar y eliminar"
2. Al seleccionar "Crear disparadores" (triggers), se conoce la información relacionada a la creación o eliminación de los mismos y de los usuarios involucrados.
3. La opción de creación de Consultas, presenta el código SQL y permite eliminar o actualizar los datos.
4. El reporte indica la máquina, el usuario, las actualizaciones realizadas en un período definido, ya sea por tablas o por columnas *(ver Fig.42)*.
5. En la barra de menú se puede apreciar: "Inicio, Auditar, Vista y Recursos".

Figura 42. ApexSQL



Fuente: [Pantallas del Programa]

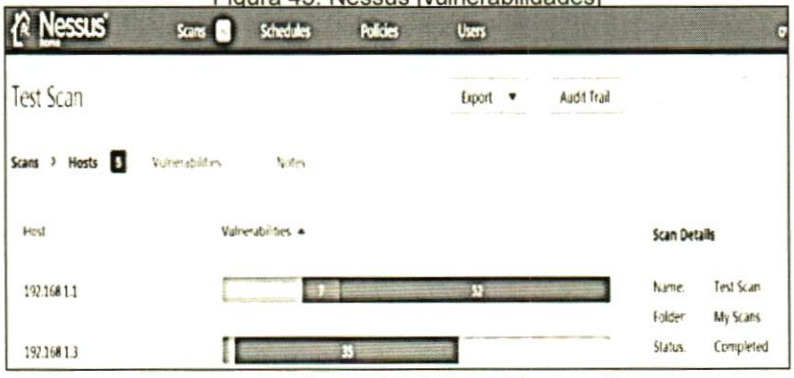
3.14. Nessus

Es un programa que detecta vulnerabilidades en la red y ofrece un análisis del nivel de seguridad, no se limita a los puertos asignados por Agencia de Asignación de Números de Internet (IANA), incluso analiza los servicios ejecutados más de una vez por un mismo cliente. Se enfoca principalmente a los controles de seguridad en la red, puede identificar anfitriones, vulnerabilidades y errores de configuración; también detecta dispositivos físicos y virtuales, sistemas operativos, aplicaciones y base de datos; asimismo, puede detectar *botnets* maliciosos, conocidos o sospechosos y combatir el *malware*. El grado de análisis puede llegar hasta la verificación de información confidencial, para cumplir con las políticas que reducen en riesgo de pérdida de datos. Finalmente, es una herramienta que se adapta a las guías del Sistema de Control y Auditoría (SCADA); en base (Nessus, 2014).

Se describe puntos del proceso de análisis:

1. Activar un código con los datos de nombre, correo electrónico y país, seleccionar el sistema operativo deseado (*Windows, Solaris, Mac OS* y *Linux*), y crear una cuenta de administrador.
2. Al iniciar el escaneo, se presenta el nombre del equipo y la última actualización, y se describen las políticas, que generalmente son: *Host Discovery, Basic Network Scan (BNS), Credentialed Patch Audit, Web Application Test. Windows Malware Scan y Mobile Device Scan.*
3. El escaneo presenta barras por cada equipo con las vulnerabilidades: "*Low, Info, y Medium*". (*Ver Fig. 43)*
4. Ofrece un reporte en *Nessus*, PDF, HTML o CSV con soluciones.

Figura 43. Nessus [vulnerabilidades]



Fuente: [Pantallas del Programa]

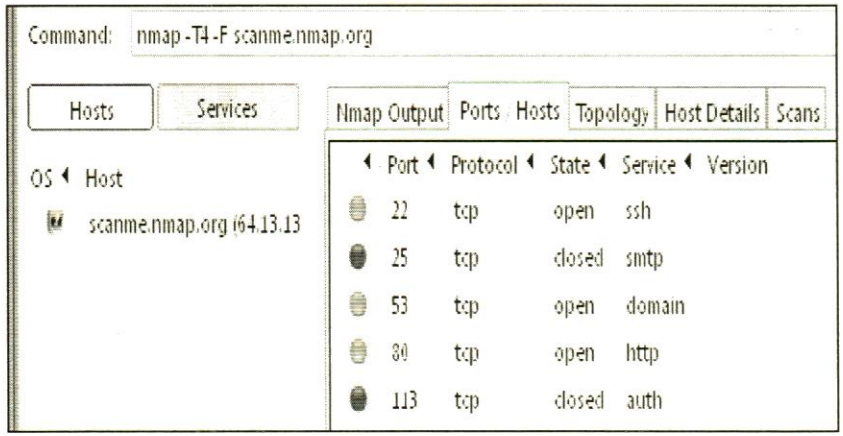
3.15. NMAP (Network Mapper)

Es un programa de código abierto y libre que permite realizar el inventario de la red o de un solo equipo conectado a *internet*, monitorea toda la actividad en tiempo real, brindando información de los sistemas operativos, filtrado de paquetes y cortafuegos activos. Trabaja de plataformas de *Linux, Windows y Mac OS*; la suite contempla una interfaz gráfica, una transferencia de datos, una herramienta de depuración, comparación del análisis de resultados y de generación de paquetes.

Se describen los puntos del proceso de análisis:

1. Inicia el escaneo con una dirección IP y se presenta información del número y tipo de puerto que se van a analizar.
2. Durante el escaneo se muestra información del puerto, protocolo, el estado "abierto o cerrado", el servicio y la versión. *(Ver Fig.44)*
3. Ofrece una gráfica de control y un reporte de puertos.
4. Incluye dos módulos "*Hosts y Services*" y las siguientes viñetas "*Output,Port/Hosts, Topology, Host Details*".
5. Ofrece la oportunidad de instalar nuevos componentes "*Nmap core Files, Register Nmap Path, Zenmap*" y otros. En base a (Nmap6.25, 2012).

Figura 44. NMAP



Fuente: [Pantallas del Programa]

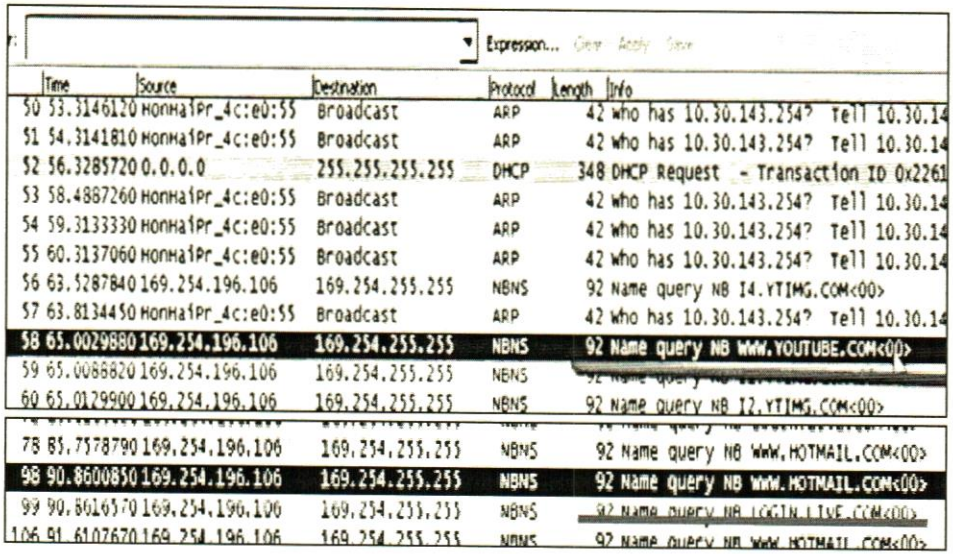
3.16. WhireShark

Es un analizador de protocolos de código abierto, disponible para las plataformas de *Windows y Unix*. Con el objetivo de capturar la actividad dentro de una red a través del tráfico de los paquetes, incluye una amplia gama de protocolos y la capacidad de filtrar la información para definir una búsqueda. Es una herramienta para conocer en tiempo real la actividad de los usuarios en la red, solo es necesario introducir la IP correspondiente, y en segundos se despliega un reporte detallado de las páginas visitadas y paquetes enviados o solicitados. Con base a (Wire Shark).

Se describen los puntos del proceso de análisis:

1. Incluye una barra de menú: *"File, Edit, View, Go, Capture, Analize, Statistic, Telephony, Tools"* y otras.
2. La pantalla principal inicia con la captura de la tarjeta de red
3. Se presenta el tráfico de red de todas las máquinas conectadas y para conocer la actividad de un equipo en específico solo es necesario introducir la IP correspondiente en el filtro de búsqueda.
4. Se observan las páginas visitadas con la dirección de origen y de destino. *(Ver Fig. 45)*.

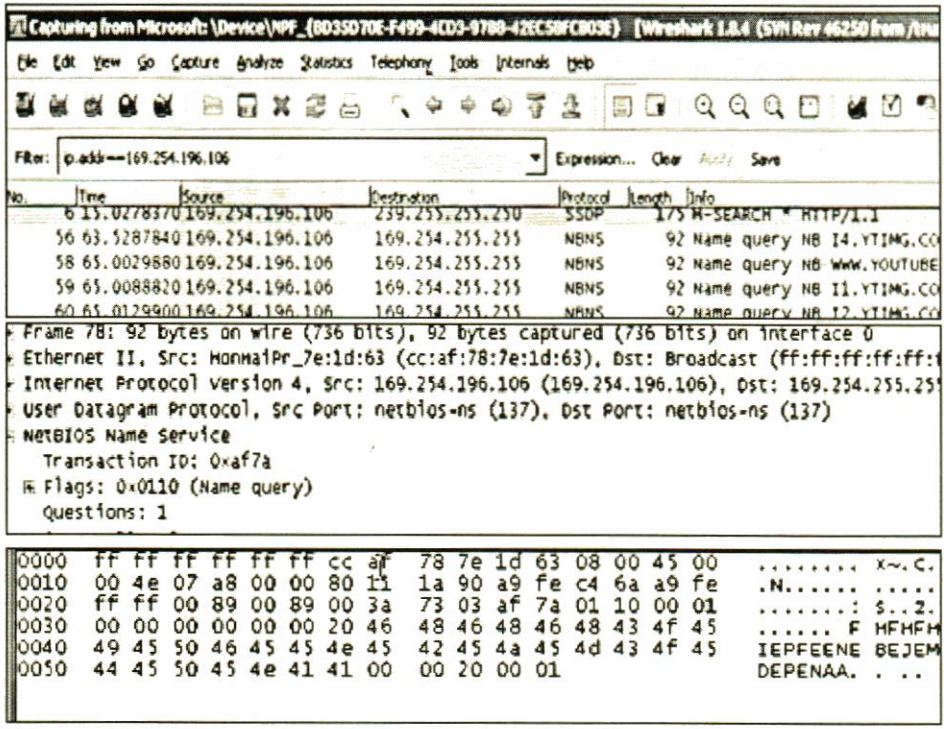
Figura 45 .WireShark



Fuente: [Pantallas del Programa]

5. El análisis se divide en tres zonas. La primera presenta el número de paquetes, tiempo, origen, destino protocolo, tamaño e información del mismo. En la viñeta de Protocolo se puede elegir entre una variedad de más de 400 protocolos existentes o anotar el Protocolo deseado en el filtro de búsqueda, está acción permite una depuración en el análisis; la segunda, es el área de captura, presenta información de un paquete en específico y la última zona, muestra la cabecera de *Ethernet*, los primeros seis dígitos de destino y seis dígitos de origen, dos *byte* del protocolo en que viaja. *(Ver Fig. 46)*.

Figura 46. WireShark [análisis]



Fuente: [Pantallas del Programa]

Una forma de rastrear con mayor detalle la actividad de un usuario en una máquina o la contraseña del mismo, es emplear la opción *Follow TCP Stream* del menú *Analyze*. Sin duda es una herramienta poderosa para evaluar la seguridad de una red.

A continuación se presenta una lista de los programas diagnósticos *(ver Fig. 47)* presentados en este capítulo y su área de seguridad informática relacionada.

Figura 47. Relación de Programas con áreas de diagnóstico

No.	Programas / Área:	SW	HW	Red	BD	WEB
1	WinAudit	✓	✓			
2	OpenAudit	✓	✓			
3	FreshDiagnose	✓	✓			
4	Lansweeper	✓	✓			
5	Total Networks Inventory	✓	✓			
6	Softkey	✓				
7	TAW					✓
8	WhatWeb					✓
9	XRumer					✓
10	Watobo					✓
11	Secure SQL Auditor				✓	
12	ApexSQL				✓	
13	NMAP			✓		
14	Nessus			✓		
15	WireShark			✓		

Fuente: [Elaboración propia]

CAPÍTULO IV

RIESGO Y CONTROL

La relación entre Riesgo y Control

Evaluación del Riesgo

Actividades de Control

Políticas de Seguridad

Cuestionario de Auditoría en Sistemas

Concentrado de Información

Resultados

4.1. La relación entre Riesgo y Control

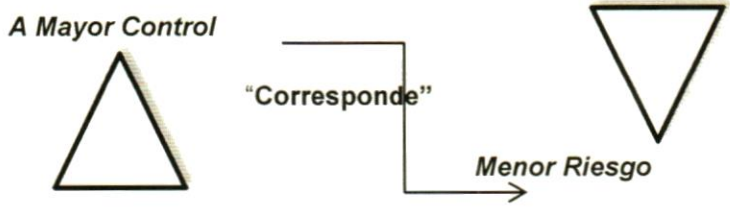
Cuando se alude al término "riesgo", invariablemente surge la "*posibilidad de que ocurra un evento no deseado*"; una forma de evitar su ocurrencia es aplicar medidas adecuadas para señalar las vulnerabilidades y reducir el grado de las amenazas.

Es cómodo pensar: *"a mí nunca me va a ocurrir" o "es cuestión de mala suerte";* lo cierto es que no importa el grado del deseo que se tenga para rechazar un riesgo, sino las medidas que se apliquen para afrontarlo.

"*Niño ahogado, pozo tapado*" es una frase coloquial para indicar que las acciones, se aplican después de que han ocurrido los accidentes. Entonces, es necesario exponer la seguridad del personal, del equipo y/o de los datos para comprender la importancia de tener un plan de acción, que estime la posibilidad de que ocurran sucesos inesperados y los costos del impacto hasta el momento en que se recupere el ritmo de las actividades.

Para la mayoría de los administradores un plan de trabajo del área de sistema que presenta un ambiente controlado es sinónimo de muchos ceros o una lista interminable de gastos para la organización; sin embargo la palabra correcta es inversión; porque garantiza la eficacia y eficiencia de las transacciones, la seguridad y confiabilidad de la información, y además ofrece un contexto reglamentado y legalizado que beneficia directamente la credibilidad y la imagen de la entidad.

No existe un sistema eternamente seguro; partiendo de la premisa de *"lo que el hombre hace, el mismo hombre deshace*"; el tiempo y la tecnología son factores importantes para la violación del sistema. Por tal motivo, es imperante lograr un equilibrio en la relación riesgo-control, tal y como se presenta a continuación:



4.2. Evaluación del riesgo

En las organizaciones, siempre se está expuesto al riesgo, algunos son más visibles o predecibles que otros; depende de la habilidad del administrador para determinar la probabilidad de ocurrencia y el impacto de las consecuencias. Por ello, antes de elaborar un Plan de Contingencia o un Plan de Continuidad, es necesario realizar una Evaluación de Riesgos (*Ver fig. 48 y 49)* que contemplan al menos, los siguientes elementos:

a) ***Vulnerabilidad***: es una debilidad o la inexistencia de un evento
b) ***Amenaza***: es el daño que puede presentarse como consecuencia
c) ***Probabilidad***: valor numérico en escala 1 a 10
d) ***Impacto***: valor numérico en escala 1 a 10
e) ***Riesgo:*** es el producto de la probabilidad X impacto, representado en porcentaje (%).
f) ***Acciones preventivas*:** estrategias para fortalecer la vulnerabilidad
g) ***Acciones correctivas*:** estrategias para reducir de la amenaza
h) ***Costo:*** contempla el gasto de implementación de las estrategias.
i) ***Plan de acción***: acciones para continuar temporalmente con las actividades mientras se restablece el control.

Figura *48.* Evaluación del Riesgo [contraseñas]

1	**Vulnerabilidad**	Contraseñas de los usuarios de correos electrónicos que no tienen un alto nivel de seguridad. (más de seis dígitos o caracteres, incluyendo letras mayúsculas y minúsculas)
	Amenaza	Ingreso y uso ilegal de la cuenta por usuarios no autorizados. Robo y violación de la privacidad de los datos
	Probabilidad	9
	Impacto	6
	Riesgo	**54%**
	Acciones Preventivas	Comprobación de datos del usuario. Actualización periódica de la contraseña (manual o automatizado). Actualización de métodos de cifrado
	Acciones Correctivas	Rastreo y cancelación de la cuenta del usuario. Crear una nueva cuenta de correo electrónico Restauración de datos
	Costo	Los costos quedan cubiertos con el salario del personal técnico, al incluir las acciones en el manual de funciones
	Plan de Acción	Proceso de restauración de cuentas y verificación de datos (tiempo aproximado: 1 hora).

Fuente: [Elaboración propia]

Figura 49. Evaluación del Riesgos [contactos eléctricos]

2	**Vulnerabilidad**	El número de contactos para el suministro de corriente eléctrica no es suficiente a la demanda de usuarios con equipos portátiles
	Amenaza	Daño físico en los contactos y en los equipos por descargas eléctricas no reguladas. En caso extremo, se puede originar un incendio provocado por el sobrecalentamiento de las líneas
	Probabilidad	9
	Impacto	8
	Riesgo	**72%**
	Acciones Preventivas	Supervisar la demanda del número de usuarios en relación al número de contactos. Aplicar las normas de seguridad en instalaciones eléctricas.
	Acciones Correctivas	Reparación de contactos dañados. Reparación o sustitución de equipos dañados por descargas eléctricas. Aplicar Plan de Contingencia en caso de incendio.
	Costo	La supervisión está incluida en las funciones del administrador del área, y la aplicación de normas de seguridad como la supervisión de las mismas, generan costos de contratación de personal experto en el área. La reparación de contactos está determinada por el número de piezas por sustituir y la reparación de los equipos depende del daño ocasionado al mismo. Los costos se elevan potencialmente en el caso de incendio y se administran en el Plan de Contingencia.
	Plan de Acción	Durante el proceso de reparación de contactos se recomienda habilitar otra área de trabajo y en el caso del mantenimiento correctivo de los equipos, se sugiere facilitar otro equipo temporalmente.

Fuente: [Elaboración propia]

El Administrador de Sistemas es el responsable de realizar estas evaluaciones y presentarlas al administrador del negocio para que en forma conjunta y en base al porcentaje obtenido en cada riesgo se determine el grado de prioridad de cada vulnerabilidad.

4.3. Actividades de control preventivo, detectivo y correctivo

Las operaciones giran en torno a los objetivos institucionales, el empleo de tecnología, infraestructura y materiales juegan un papel muy importante para su aplicación, asimismo es indispensable la intervención del recurso humano para la obtención de resultados oportunos y exactos.

Pero una medida necesaria es el cumplimiento de los controles administrativos aplicables al negocio.

Las actividades de control permiten a los responsables de cada operación realizar sus funciones con la certeza de estar protegidos y preparados para actuar en el momento en que ocurra un suceso inesperado. Los controles pueden clasificarse en:

a) ***Preventivos***: ayudan a reducir las vulnerabilidades y eliminar las causas que originan un acto no deseado "Riesgo".
b) ***Detectivo:*** su función no es prevenir, si no detectar cuando el riesgo está presente y evaluar la eficacia de los controles internos.
c) ***Correctivo:*** a toda causa de riesgo corresponde una consecuencia que amenaza el correcto funcionamiento de las operaciones, la reparación de los errores puede ser un trabajo difícil y tardado, si no se tienen contemplado los controles que se deben aplicar.

A continuación se presentan tres ejemplos de controles *(ver fig.50, 51 y 52)*

Figura 50. Actividades de Control [acceso a BD]

Control	**Para el acceso a las bases de datos.**
Preventivo	Crear respaldos y actualizarlos periódicamente. Asignar responsabilidades por escrito a las personas que tienen acceso autorizado a las bases de datos. Estipular las reglas asociadas con el acceso a la información y las consecuencias por la pérdida o mal uso de la misma. Utilizar sistemas para monitorear y detectar actividad sospechosa.
Detectivo	Colocar un programa que administre automáticamente los cambios en la base de datos documentando y reportando excepciones hechas a las base de datos diariamente para proveer rastreo y monitoreo profesional que permita identificar al responsable de una actividad sospechosa. Registrar datos de los usuarios que realicen extracciones de datos digitales de las bases de datos que tienen información sensible y revisar cada acción periódicamente.
Correctivo	Examinar las debilidades del sistema, procedimiento o recurso que se está utilizando, para que no ocurra esta situación de nuevo, tratando de corregir rápidamente, antes de que se presente otro ataque a la seguridad. Recuperar los respaldos. Actuar conforme a la Ley sobre datos sensibles.

Fuente: [Elaboración propia]

Figura 51. Actividades de control [pérdida de datos]

Control	Para evitar la pérdida de datos ante una interrupción eléctrica.
Preventivo	Instalar UPS en los equipos de cómputo previamente cargados, con el fin de prevenir la pérdida de archivos al momento de estar trabajando.
Detectivo	Los Ups entran en acción al momento de existir una deficiencia de corriente, el único problema es el lapso tiempo que los ups son capaces de soportar, el trabajo de las maquinas varía de 20 a 30 minutos.
Correctivo	Poner a funcionar una planta de corriente auxiliar, puesto que es un centro de cómputo y no deben haber interrupciones

Fuente: [Elaboración propia]

Figura 52. Actividades de Control [tráfico de red]

Control	Para monitorizar el tráfico de una red y detectar intrusos.
Preventivo	Utilizar un rango de direcciones con entradas validas en las tablas de ruteo de la organización, y que todo el tráfico que entra por este espacio de direcciones sea considerado sospechoso. Utilizar un *firewall* para prevenir que los *honeypot* intrusos, puedan tener acceso a las demás computadoras de la organización, en donde el tráfico de entrada sea libre y el tráfico de salida limitado.
Detectivo	Utilizar un IDS (sistemas detectores de intrusos), así como monitores de red para ver la actividad de los *honeypot*. Detectar y aprender las técnicas que se utilizaron por parte de los intrusos, para utilizar esta información.
Correctivo	Es aplicado hacia los *honeypot* que fueron violados por los intrusos; se vuelven a programar para corregir los fallos de seguridad, tomando en cuenta las técnicas que emplearon los atacantes para acceder.

Fuente: [Elaboración propia]

Honeypot: es un sistema o unidad de datos preparado como trampa para detectar ataques y aprender la metodología usada en éstos, además de guardar rastro forense del atacante para efectos legales cuando sea posible (Maulini). El administrador del Centro de Cómputo o del Área de Sistemas es el responsable de realizar las actividades de control.

4.4. Políticas de seguridad informática

Las políticas dentro de una organización son una medida de control, que al ser aplicadas correctamente disminuyen la probabilidad de ocurrencia

del riesgo, brindando seguridad en la actuación de las personas; siempre y cuando, éstas sean publicadas, difundidas, actualizadas y aplicadas conforme a lo establecido.

Las personas asignadas para la elaboración de las políticas deben de tener la capacidad para detectar vulnerabilidades, la habilidad para redactar los enunciados en forma sencilla, clara y pertinente, sin confusiones ni tecnicismos.

Pertenecer a un grupo interdisciplinario y representativo del nivel operativo, administrativo y gerencial, para mantener una relación estrecha con los objetivos y metas del negocio.

Una política señala un objetivo, el cual debe de estar descrito explícitamente para su correcta aplicación; es importante señalar las excepciones y especificaciones por medio de corchetes [ ], dentro del enunciado para que no exista o provoque una interpretación inadecuada o ventajosa; en casos particulares definir la sanción correspondiente.

Para una mejor explicación, se citan a continuación 10 políticas de seguridad:

1. **De acceso al sistema**. Todo usuario dispondrá de autorización de acceso al sistema compuesta por el identificador personal y contraseña correspondiente, la cual será asignada exclusivamente por el Administrador del área de Sistemas y entregada al responsable siguiendo el protocolo de seguridad.
   [La contraseña la genera un sistema en forma aleatoria y se modifica cada 30 días en forma permanente y el protocolo de seguridad consiste en la entrega personalizada y confidencial de la contraseña].

2. **Contenido de información**. La información de cada equipo, es responsabilidad de cada usuario designado por la organización; por lo tanto no se permiten archivos de carácter personal o no autorizados para el desarrollo de sus funciones.
   Esta falta administrativa por considerarse de alto impacto al rendimiento laboral y equipo, amerita una sanción que implica el despido inmediato del personal, respetando las disposiciones laborales.
   [Los archivos no autorizados se refieren a datos, música, video y fotografías; asimismo respaldos o programas ejecutables].

3. **De instalación de *software*.** Todo *software* instalado en las computadoras es acreditado por las estrategias institucionales; por lo tanto, está prohibida la instalación de cualquier otro programa o aplicación, y en caso de ser necesario para las actividades laborales, se deberá contactar con el administrador de sistemas para su evaluación, aceptación y correspondiente instalación.
   [El Software no acreditado se refiere a los reproductores de imágenes, música, aplicaciones sociales y de entretenimiento].

4. **Uso del *internet*.** El empleo del *internet* está restringido a las páginas institucionales, queda estrictamente prohibido navegar en sitios no autorizados.
   Al personal que sea identificado por el sistema de rastreo, se sancionará con el despido inmediato, respetando las cláusulas conforme a la Ley, por considerarse una falta administrativa de alto impacto al rendimiento laboral y al equipo.
   [Los sitios no autorizados se refieren a las redes sociales, reproductor de música y videos, navegadores, buscadores y páginas con contenido pornográfico; el rastreo de IP indica el historial de navegación y las páginas visitadas en tiempo real por cada usuario]

5. **Uso del correo electrónico.** El servicio de mensajería electrónica es únicamente a través del correo institucional y para funciones estrictamente laborales, queda prohibido el uso personal del servicio, el envío y revelación de datos sensibles de la institución, de las personas que la integran, o que estén relacionadas hacia terceros.
   La falta a esta política, penaliza al responsable conforme a lo establecido en el Código Penal por violaciones a las leyes de protección de datos personales, de derechos de autor, de propiedad industrial y de protección al consumidor.
   [Los datos sensibles pueden ser marcas patentadas, secretos industriales, obras protegidas por derechos de autor y datos personales]

6. **Ubicación de los equipos.** Se indica a todos los usuarios y personas de esta organización, que el cambio de lugar de los equipos de cómputo, de comunicación y dispositivos, es una actividad exclusiva del personal autorizado, obedeciendo a los intereses institucionales para obtener el mayor rendimiento de los mismos.

El daño ocasionado al equipo por la falta de observación de esta política será cubierta al 100% por el usuario.
[El personal autorizado puede ser administrador del área de sistemas, técnicos y asistentes]

7. **Uso de dispositivos de almacenamiento**. Para protección de los equipos y de la información, está prohibido el uso de cualquier dispositivo de almacenamiento.
   Cuando el usuario requiera transferir o respaldar información deberá solicitar la autorización y aprobación del administrador del área de sistemas.
   El usuario que sea detectado por el sistema de bloqueo de puertos, será penalizado conforme a las disposiciones legales, en relación al registro de actividades realizadas en el equipo.
   [Los dispositivos de almacenamiento pueden ser: usb, memory stick, memory card, cd, dvd, discos duros portables, y otros]

8. **Horario de servicio.** Los usuarios pueden disponer de servicio del equipo siempre y cuando se encuentre dentro del tiempo estipulado por el horario oficial.
   El usuario que sea detectado por el sistema de rastreo y vigilancia, fuera de los horarios establecidos, será sancionado, en relación al registro de las actividades realizadas en el equipo.
   [Los usuarios que requieran el equipo para realizar actividades institucionales emergentes fuera del horario de servicio estipulado, deberán solicitar la autorización y aprobación del administrador del área de sistema]

9. **Introducir alimentos**. En el área de Centro de Cómputo y Servidores, queda prohibido introducir e ingerir bebidas, alimentos y cualquier tipo de aperitivos o dulces.
   [El usuario que se le sorprenda faltando a esta política será retirado del área y cancelada su contraseña de acceso].

10. **Cierre de sesión**. Los usuarios tienen la obligación de cerrar cada sesión de trabajo, asimismo, el usuario debe colaborar en apagar los equipos para contribuir con el ahorro de energía eléctrica y conservación ambiental.
    El administrador del área de sistemas y sus colaboradores no son responsables por transacciones pendientes, al momento de cerrar sesiones que quedaron abiertas.

4.5. Cuestionario de Auditoría en Informática

Una forma de obtener información en una investigación, es contar con un instrumento de recolección de datos que permita la medición del control y el riesgo existente en el área de estudio, basado en temas de interés específicos.

A continuación se presentan 100 preguntas distribuidas en tres rubros para medir temas de interés en cada uno de ellos:

1. **Tecnología:** *software, hardware* y redes
2. **Gestión administrativa**: recursos humanos y procedimientos
3. **Recurso físico:** infraestructura y materiales

Existe una gran diversidad de criterios de cuestionarios, pero en base al objeto de estudio, se enfocan preguntas cerradas y respuestas categorizadas con escala de valores diferentes, con un diseño cualitativo y cuantitativo.

a) Cualitativo; presenta tres características referenciadas por los incisos A), B) o C) de las cuales únicamente pueden seleccionar una opción. Las respuestas se encuentran ordenadas con una escala de mayor a menor prioridad. A)=3 puntos, B)=2 puntos y C)=1 punto; y

b) Cuantitativo; presenta varias características y pueden seleccionarse más de una opción, marcando la respuesta elegida en cada recuadro (☑). No incluye prioridad y guarda la siguiente relación: "A mayor número de aciertos, mayor puntuación", pero la puntuación máxima es de 3 puntos distribuidos en todas las respuestas, esto para mantener el equilibrio con las demás preguntas.

La redacción de las preguntas mantiene un lenguaje sencillo, preciso, lógico, y neutral; contiene tecnicismos propios del área de sistemas.

No incluye respuestas abiertas para mantener un enfoque imparcial, estandarizado y para facilitar posteriormente la interpretación, codificación y programación del cuestionario.

Se recomienda ser llenado por el auditor en relación a la observación y análisis de evidencias presentadas.

4.5.1. Tecnología

a) Software

1. Las licencias de *software* instalado en los equipos son:
   A) Privadas/gratuitas
   B) De pruebas
   c) Craqueadas

2. Tipo de sistema operativo instalado en los servidores:
   A) Unix
   B) Windows
   C) Linux

3. Tipos de sistemas operativos instalados en los equipos de cómputo, (no precisamente en el mismo):

   ☐ Windows ☐ Solaris

   ☐ Linux

4. Los recursos de *software* instalados para funciones básicas son:

   ☐ Procesador de texto, ☐ Editor de folletos,

   ☐ Hoja de cálculo, ☐ Editor de tutoriales,

   ☐ Base de datos, ☐ navegadores,

   ☐ Editor presentaciones, ☐ buscadores

   ☐ Editor de videos,

5. Los recursos de *software* instalados para funciones de limpieza del sistema detectan y eliminan:

   ☐ *Adwares* (programas que presentan anuncios publicitarios)

   ☐ *Spyware* (programas que espían las páginas visitadas)

   ☐ *Malware* (programas que se infiltran para robar datos)

   ☐ Virus, (programas maliciosos)

   ☐ Troyanos (programa malicioso-enmascarado)

- ☐ Gusanos (programa malicioso que se reproduce)

6. Los recursos de *software* instalados para la administración del sistema, atienden:
   - ☐ El rendimiento de la memoria virtual y memoria cache
   - ☐ La asignación de privilegios y funciones de usuarios
   - ☐ La supervisión de actividades en una red local o remota.
   - ☐ Otros

7. *Software* instalado para la administración de base de datos:
   A) Oracle
   B) Postgressql /SQL Server
   C) Access/Mysql/foxpro

8. [SISTEMA]. Periodicidad con que se realiza un análisis de virus:
   A) Semanal
   B) Mensual
   C) Diferente a las anteriores

9. [SISTEMA]. Periodicidad con que se realiza el cambio de contraseñas:
   A) Semana
   B) Mensual
   C) Diferente a las anteriores

10. [SISTEMA]. Método que se emplea para el control de acceso lógico:
    A) Método biométrico
    B) Contraseñas de acceso
    C) Diferente a las anteriores

11. [SISTEMA]. El control de equipo por usuario, se realiza por medio de:
    A) Programa automatizado
    B) Forma manual
    C) Diferente a las anteriores

12. [BASE DE DATOS]. Periodicidad con que se respaldan los datos:
    A) Diario
    B) Semanal
    C) Diferente a las anteriores

13. [BASE DE DATOS]. Estrategias de seguridad que se emplean en el control de transacciones:

- ☐ Mediante *software* de auditoría BD (p.e. SQLAUDITOR)
- ☐ Líneas de código para definición de restricciones de integridad
- ☐ Líneas de código para el control de concurrencia (candados, disparadores, etc.)
- ☐ Protocolos en recuperación de datos
- ☐ Permisos en cuentas de usuarios (privilegios)

14. [BASES DE DATOS]. Protocolo de seguridad, empleado para la recuperación de información:

- ☐ Contratación de servicios externos (outsourcing)
- ☐ A nivel software (Recuva, Easy Drive Data Recovery)
- ☐ A nivel código: técnicas de recuperación(paginación de Sombra, RAID)

15. [BASES DE DATOS]. Tipos de datos de carácter personal clasificados de ALTO riesgo, que son protegidos por el sistema:

- ☐ Ideología
- ☐ Origen racial,
- ☐ Religión
- ☐ Salud,
- ☐ Creencias,
- ☐ Vida sexual

16. [BASE DE DATOS]. Tipos de datos de carácter personal clasificados de MEDIO riesgo, que son protegidos por el sistema:

- ☐ Infracciones penales
- ☐ Datos fiscales
- ☐ Infracciones administrativas
- ☐ Servicios financieros

17. [BASE DE DATOS]. Tipos de datos de carácter personal clasificados de BAJO riesgo, que son protegidos por el sistema:

- ☐ Nombre
- ☐ Edad
- ☐ Dirección
- ☐ sexo

18. [INTERNET].Periodicidad en que se aplican los protocolos de seguridad.
    A) Diario
    B) Semanal
    C) Diferente a las anteriores

19. [INTERNET]. El protocolo de seguridad incluye la depuración de :
    - ☐ Cookies (registros temporales de páginas visitadas)
    - ☐ Spam (mensajes de publicidad no solicitadas)
    - ☐ Phishing (páginas falsas para robar datos a través del engaño)
    - ☐ Virus (programas maliciosos)

20. [INTERNET]. Estrategias de seguridad que se emplean para la protección de los datos en la página WEB:
    - ☐ Certificados de seguridad
    - ☐ Pruebas de vulnerabilidad con inyección SQL
    - ☐ Mediante Software de auditoría WEB (p.e. WATOBO)

21. [INTERNET] El Monitoreo y supervisión de actividades en la Web, que realizan los usuarios en los equipos, es a través de:

    A) Software automatizado
    B) Vigilancia personal
    C) Diferente a las anteriores

b) Hardware

22. Promedio de capacidad de memoria RAM que tienen las computadoras:

    A) 16 Gb
    B) 8 Gb
    C) 4 Gb

23. Promedio de capacidad de Disco Duro que tienen las computadoras:

    A) Mayor o igual a 500Gb
    B) 300 a 400 Gb
    C) Menor o igual a 200 Gb

24. Los componentes que incluyen la mayoría de las computadoras son :

- ☐ Tarjeta de red
- ☐ Tarjeta de video
- ☐ Tarjeta de sonido
- ☐ Tarjeta inalámbrica

25. Los puertos o unidades lectoras que incluyen la mayoría de las computadoras son:

- ☐ USB,
- ☐ Discos ópticos,
- ☐ Memoria micro SD,
- ☐ Cintas flexibles
- ☐ Memoria stick,

26. El dispositivo de almacenamiento que se emplea para los respaldos de las BD:

A) Cinta magnética
B) Disco duros o discos ópticos
C) Memorias extraíbles

27. Medidas de seguridad que se aplican a los dispositivos USB que ingresan a las computadoras:

- ☐ Aplicar el Software antivirus a las USB candidatas
- ☐ Detección y eliminación de software "roba-datos" de las USB candidatas
- ☐ Ingreso solo USB autorizadas, que contenga la contraseña del programa de seguridad.(p.e. RohoslogonKey/IdUsbLockKey)

28. A que recursos de *hardware* se le realiza mantenimiento preventivo:

- ☐ Servidores
- ☐ proyectores,
- ☐ Equipo de cómputo,
- ☐ impresoras,

29. Periodicidad con que se realiza el mantenimiento preventivo:

A) 6 meses
B) Un año
C) Diferente a las anteriores

30. Protocolo ambiental para el tratamiento de los residuos de cómputo:

    A) Los equipos son enviados a empresas de reciclaje tecnológico
    B) Los equipos son depurados y se extraen las piezas que pueden ser reemplazables y útiles en otros equipos
    C) Diferente a las anteriores

31. Protocolo que emplean para la destrucción de los dispositivos de almacenamiento y la información contenida.

    A) Contratación de empresas con servicio de destrucción
    B) Electroimán, exposición intensa al calor.
    C) Formateo o enviarlo a la basura local

c) Redes

32. Tipo de conexión que se ocupa en la red:

    A) Inalámbrico
    B) Cableada
    C) No hay conexión

33. La asignación de las IP a los equipos de red es:

    A) Estática
    B) Dinámica
    C) Sin asignación

34. Los controles de acceso para la conexión a *internet*, es por medio de:

    A) Firewall
    B) Proxy
    C) DNS/DHCP

35. La asignación de la IP para los servidores es:

    A) Pública
    B) Privada
    C) Sin asignación

36. El material de las vías de acceso es :

    A) Fibra óptica
    B) Radio: WLL, MMDS, LMDS
    C) Diferente a las anteriores

37. El tipo de encriptación para la red inalámbrica es:

    A) WPA2 / WPA
    B) WEP / FILTRADO MAC
    C) Diferente a las anteriores

38. El protocolo empleado para enviar datos a tu base de datos es:

    A) HTTPS
    B) HTPP
    C) Diferente a las anteriores

4.5.2. Gestión Administrativa

a) Recurso Humano

39. ¿Qué personal integra el área de sistema?

    ☐ Administrador del Centro de Cómputo
    ☐ Administrador de Redes y Comunicaciones
    ☐ Administrador de Base de Datos
    ☐ Analista, Programadores y Capturista.
    ☐ Técnico en mantenimiento de equipos
    ☐ Auditor de Seguridad

40. Perfil académico del responsable del área de sistema:

    A) Maestría en Sistemas
    B) Licenciatura en Sistemas
    C) Técnico en Sistemas

41. Funciones más importantes del área de sistema.

- ☐ Control de usuarios
- ☐ Control de equipo de cómputo
- ☐ Control del personal
- ☐ Control Comunicaciones
- ☐ Control de Rec. Materiales
- ☐ Desarrollo de Programas
- ☐ Mantenimiento Preventivo/Correctivo
- ☐ Seguridad

42. Antigüedad comprobable del responsable en el área de Sistemas (Título y Cédula profesional)

A) Más de 5 años
B) menos de 5 años
C) menos de un año

43. Conocimientos comprobables del responsable en el área de Sistemas:

- ☐ Redes y Comunicaciones
- ☐ Mantenimiento de Hardware
- ☐ Diseño y Programación
- ☐ Seguridad de sistemas

44. Documentos probatorios del responsable en el área de Sistemas.

- ☐ Título profesional
- ☐ Cédula Profesional
- ☐ Certificación
- ☐ Diplomas/Constancias

45. Habilidades del responsable en el área de Sistemas

- ☐ Dirección,
- ☐ Administración
- ☐ Operativas
- ☐ Comunicación

46. Personal que realiza el servicio de mantenimiento preventivo / correctivo:

A) Contratación externa (outsourcing)
B) Personal técnico responsable
C) El mismo personal del área de sistema

47. Personal que realiza los respaldos de las BD

A) Contratación externa (outsourcing)
B) Administrador Centro de Cómputo
C) Diferente a las anteriores

48. Los indicadores que se emplean para medir las habilidades de los analista y programadores son:

- ☐ Iniciativa y creatividad Respuesta bajo presión,
- ☐ Manejo de múltiples tareas
- ☐ Coordinación y compromiso con el equipo de trabajo.
- ☐ Responsabilidad y puntualidad
- ☐ Asistencia y buena presentación

49. Para medir el desempeño laboral de los analistas/programadores, es necesario presentar documentación que supervise los siguientes aspectos:

- ☐ Productividad; presenta el número de proyectos "terminados o en proceso", en los cuales participa y los módulos que realiza.
- ☐ Rendimiento: presenta el cumplimiento de las actividades desarrollas en tiempo real o tiempos de holgura.
- ☐ Calidad; presenta el número de pruebas realizadas a los proyectos antes y después de terminados, el número de usuarios participantes y los resultados obtenidos.
- ☐ Institucional; presenta el número de documentos entregados, en cumplimento a los procedimientos institucionales.

c) Procedimientos

50. Documentos existentes para el control administrativo en el área de sistemas

- ☐ Políticas de Contratación
- ☐ Proyecto de Trabajo
- ☐ Manual de procedimientos
- ☐ Manual de Funciones
- ☐ Reglamento de Servicio
- ☐ Organigrama

51. Documentos para el control operativo en el área de sistemas

- ☐ Diagrama de Red.
- ☐ Planos instalación eléctrica
- ☐ Planos instalación hidráulica
- ☐ Planos arquitectónicos.

52. Documentos relacionados al control administrativo y operativo:

- ☐ Se difunden
- ☐ Se actualizan
- ☐ Son Pertinentes
- ☐ Se aplican

53. Estrategias de evaluación de procedimientos internos del área:
   A) Alguna de las tres: Auditoría de informática, de Sistemas, en Programa
   B) Cualquiera de las dos: reportes o buzón de quejas y sugerencias
   C) No se evalúa

54. El Control de contraseñas se actualiza:
   A) Periódicamente: Cada semana o cada mes
   B) Eventualmente: Cada año o más de un año.
   C) Esporádicamente: Cuando lo requiera el usuario o nunca.

55. El control de "equipo", presenta los siguientes datos:

- ☐ Horas de uso por equipo
- ☐ Servicios más recurrentes
- ☐ Horas de uso por usuario
- ☐ Software más solicitados

56. El control de "usuario", presenta los siguientes datos:

- ☐ Registro del usuario
- ☐ Actividades realizadas
- ☐ Número de máquina/IP
- ☐ Día y hora

57. El control para el uso de dispositivos USB, memorias y discos portables que ingresan en los equipos, presenta los siguientes datos:

- ☐ Fecha y hora de ingreso
- ☐ Archivos extraídos
- ☐ Archivos enviados
- ☐ Ruta Origen/Destino
- ☐ Nombre y firma de quién realiza.
- ☐ Nombre y firma de quién autoriza

58. El control de los respaldos de las Bases de Datos (Backup), presenta los siguientes datos:

- ☐ Folio de los archivos
- ☐ Fecha y hora
- ☐ Folio del dispositivo
- ☐ Nombre y firma del responsable

59. La ubicación de los respaldos de la información por medidas de seguridad es:
    A) En la NUBE (Could files)
    B) Afuera de las Instalaciones y/o del área de Servicio
    C) Diferentes a las anteriores.

60. El inventario de cómputo debe incluir los siguientes Equipos.

- ☐ Software Hardware
- ☐ Red y comunicaciones
- ☐ Equipo multimedia
- ☐ Equipo de presentación
- ☐ Mobiliario (sillas y mesas)

61. El inventario de *software*, debe presentar los siguientes datos:

- ☐ Id producto
- ☐ Id proveedor
- ☐ Nombre producto
- ☐ Descripción
- ☐ Fecha de instalación
- ☐ Fecha última actualización

62. El inventario de *hardware*, debe presentar los siguientes datos:

- ☐ Número de equipo,
- ☐ Número de serie
- ☐ Marca del proveedor
- ☐ Color del equipo
- ☐ Estado actual del equipo "funciona" o "No-Funciona"
- ☐ Encabezado: [nombre del área, nombre del responsable del área, fecha y hora de inventario]
- ☐ Pie de página:[nombre de la persona que realiza el inventario y nombre de quien lo aprueba]

63. Las adquisición de *software* se realiza obedeciendo los lineamientos de la institución en atención a:

- ☐ Usuarios
- ☐ Proveedores
- ☐ Administradores del área.
- ☐ Administradores del negocio

64. La elección del proveedor, se basa en el cumplimiento de los siguientes aspectos:

- ☐ Presentación
- ☐ Adiestramiento
- ☐ Servicio de Asesoría
- ☐ Garantía o Seguro
- ☐ Escalabilidad del producto
- ☐ Prestigio de la marca.

65. Documentos relacionados al diseño y desarrollo de Programas de Aplicación:

- ☐ Manual de usuarios,
- ☐ Diagramas E-R
- ☐ Diagrama de Flujo
- ☐ Códigos
- ☐ Catálogos de sistemas

66. Los Programas de Aplicación *WEB* que se desarrollan en el área, cumplen con las siguientes normas:

- ☐ Ley de Protección de Datos Personales en posesión de los particulares, Capítulo II (art 6° a art 21°)
- ☐ Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, Capítulo IV (art 20° al art 26°)
- ☐ Ley Federal de Telecomunicaciones, Capítulo IV. (art 41° al art. 49°)
- ☐ Ley Federal de Derechos de Autor (art 101° al art 114°)
- ☐ Ley Federal de Protección al Consumidor, Capítulo VIII BIS (art. 76°)
- ☐ Código Penal, Capítulo I (art 210° - art 211°)

67. En caso de una emergencia, se cuenta con:

- ☐ Plan de Riesgo
- ☐ Plan de Contingencia
- ☐ Plan de Continuidad

68. En el tema de prevención de una amenaza, se realizan las siguientes acciones

- ☐ Capacitación del personal
- ☐ Adiestramiento del personal
- ☐ Simulacros

69. Los Planes de Riesgo, Contingencia y/o Continuidad:

- ☐ Se difunden
- ☐ Se actualizan
- ☐ Son pertinentes
- ☐ Se aplican

70. Riesgos que se incluyen en los planes anteriores:

- ☐ Virus
- ☐ Robo de información y/o equipo.
- ☐ Accesos no autorizados al sistema / instalaciones
- ☐ Fallas eléctricas
- ☐ Desastres naturales
- ☐ Incendio
- ☐ Fraude
- ☐ Filtración por Internet
- ☐ Fallas de Conexión a Internet
- ☐ Daño físico a dispositivos de almacenamiento y respaldo.
- ☐ Vandalismo
- ☐ Políticas inexistentes

71. Elementos del Plan de Riesgos

- ☐ Una lista de posibles Riesgos
- ☐ Una lista de posibles amenazas/ vulnerabilidades en relación al riesgo.
- ☐ Porcentaje de probabilidad de ocurrencia
- ☐ Acción preventiva
- ☐ Acción correctiva

- ☐ Impacto económico de la amenaza
- ☐ Costo de acción preventiva
- ☐ Costo de acción correctiva

72. Elementos del plan de contingencia:

- ☐ Acciones en la emergencia
- ☐ Tiempo estimado en la ejecución de cada acción
- ☐ Responsable de cada acción
- ☐ Costo estimado

73. Elementos del plan de continuidad:

- ☐ Acciones temporales para continuar trabajando
- ☐ Acciones para evaluar los daños
- ☐ Acciones para la recuperación de daños
- ☐ Acciones para elaboración de recomendaciones
- ☐ Responsables de cada acción

4.5.3. Recursos físicos

a) Infraestructura

74. Área física (mts$^{2)}$ por persona:

A) 3 mts^2 por personas
B) 2 mts^2 por personas
C) 3 mts^2 por personas

75. Material de construcción del área de sistemas

A) Concreto
B) Paneles/ plafones
C) Madera/tabla roca

76. El área de sistemas está ubicada en una zona, que evita los riesgos de:

- ☐ Incendio
- ☐ Sismo
- ☐ Inundación
- ☐ Interferencia radar
- ☐ Vandalismo
- ☐ Contaminación

77. Medidas de prevención en caso de un incendio

- ☐ Alarma contra incendio
- ☐ Puertas de emergencia con acceso disponible.
- ☐ Extintores, bocas de incendio equipadas (mangueras).
- ☐ Detectores de humo
- ☐ Pintura no inflamable
- ☐ Pared no inflamable
- ☐ Piso no inflamable
- ☐ Techo no inflamable

78. Medidas de prevención en caso de un desastre natural (temblor, inundación, huracán)

- ☐ Simulacros de prevención
- ☐ Alarmas sonoras y audibles
- ☐ Puertas de emergencia con acceso disponible
- ☐ Puntos de reunión de protección civil
- ☐ Señalamientos visibles
- ☐ La ubicación del centro de cómputo exento a los efectos de un desastre natural

79. Medidas de prevención en caso de vandalismo y actividades ilícitas.

- ☐ Cámaras de vigilancia
- ☐ Ubicación del centro de cómputo aislado del tránsito continúo de personas ajenas a la institución
- ☐ Evitar ventanales de cristal que permitan una gran visibilidad del área y de los equipos

- ☐ Disponer de puertas con cerraduras y protección en las ventanas
- ☐ Caseta de vigilancia para el control de personal ajeno a la institución

80. Relación de contactos por computadoras:
   A) 1 contacto por equipo
   B) 1 contacto por cada 2 equipos
   C) 1 contacto por 3 o más equipos

81. Tipo de instalación de los contactos

- ☐ Oculta
- ☐ Entrada trifásica
- ☐ Polarización

82. Porcentaje de funcionalidad de los contactos
   A) 80% al 100%
   B) 50% al 79%
   C) 0%-49%

83. Características del cable:

- ☐ Número 12
- ☐ 220 V
- ☐ Bicolor

84. Mecanismos de prevención, sí la fuente de corriente alterna es interrumpida por sobrecarga de voltaje:
   A) Se activa la planta de energía privada
   B) Los supresores de pico, reguladores no-break, brindan un tiempo de holgura
   C) Los reguladores evitan el daño de la sobrecarga, pero el equipo se apaga inmediatamente

85. Características de la fuente de corriente eléctrica para el área de sistemas

- ☐ Es independiente a otras áreas de la institución
- ☐ Está protegida para evitar el acceso a personas no autorizadas

☐ Se realizan rutinas de evaluación de cargas

☐ Tiene instalación de tierra física

86. Se realiza mantenimiento preventivo de:

☐ Mesas ☐ Pisos

☐ Sillas ☐ paredes

87. Son los espacios que existen de apoyo al Centro de Cómputo:

☐ Servidores ☐ Almacén

☐ Bodega ☐ Taller de Mantenimiento

b) Materiales

88. Tipo de ventilación en el área de sistema

A) Aire acondicionado
B) Ventiladores
C) Ventanales

89. Cantidad de BTU por metro^2 y por zona, que brinda el aire acondicionado:
Escribir metro^2: _____ y Zona: _____y comparar con la tabla (*ver fig.53)*.

A) Cumple correctamente con lo descrito
B) Cumple con una unidad menos.
C) Cumple con dos o más unidades menos

Figura 53. BTU por mt^2 y por zona.

Mts ^{2}	Zona 1	Zona 2	Zona 3	Zona 4
0 a 4	6000 BTU	5400 BTU	6600 BTU	7200 BTU
4 a 8	8000 BTU	7200 BTU	8800 BTU	9600 BTU
8 a 12	10000 BTU	9000 BTU	11000 BTU	12000 BTU
12 a 16	12000 BTU	10800 BTU	13200 BTU	14400 BTU
16 a 20	14000 BTU	12600 BTU	15400 BTU	16800 BTU
20 a 25	18000 BTU	16200 BTU	19800 BTU	21600 BTU
25 a 30	24000 BTU	21600 BTU	26400 BTU	28800 BTU

Fuente [basado en, Quecalor.com]

Zona 1: Aguascalientes, Colima, Guanajuato, Jalisco, Nayarit, Tlaxcala, Zacatecas
Zona 2: DF. Edo Mex. Hidalgo, Michoacán, Morelos, Puebla, Querétaro,
Zona 3: BCS, Guerrero, Oaxaca, SLP, Veracruz
Zona 4: BCN, Campeche, Chiapas, Chihuahua, Durango, Quintana Roo, Sinaloa, Sonora, Tabasco, Yucatán y Nuevo León.

90. Requisitos que cumplen los aires acondicionados, instalados en el área de cómputo:

- ☐ Ductos limpios,
- ☐ Exentos de ruidos,
- ☐ Instalados a mínimo un metro de los equipos
- ☐ Disponibilidad para el control de temperatura

91. Tipo de Extintores en el área de sistemas (*ver Fig. 54).*
A) Gas Halotron
B) CO 2 / polvo
C) Agua / no tiene
D)

Figura 54. Tipos de extintores

Polvo	Es el más común, son de color rojo y en la parte frontal cuentan con una etiqueta indicando la última fecha de recarga.
CO 2	Es gas frío para incendios en equipos delicados, de color rojo, que no cuenta con manómetro.
Gas Halotrón	Para equipo de cómputo, comúnmente en color verde
Agua a presión	Color blanco o de acero inoxidable
Agua AFFF	extintores de espuma, color blanco o de acero inoxidable

Fuente: [basado, Extintores Nacionales]

92. Características del extintor

- ☐ Ubicado dentro del área de cómputo
- ☐ Portable
- ☐ Máximo 20 Kilogramos.

☐ Acceso disponible

☐ Equipo disponible (sin llave)

93. Tipo de mesas y sillas disponibles para el equipo de cómputo

A) Mesas con sillas (individual)
B) Mesas binaria con dos sillas
C) Mesa comunitaria con varias sillas.

94. Material de fabricación de mesas

A) Tubería en las patas, lámina y madera aglomerada
B) De madera
C) Triplay/melanina/formaica

95. Material de fabricación de sillas

☐ Altura graduable

☐ Acojinada

☐ Ergonómica

96. Tipo de fabricación de lámparas

A) Halógeno
B) Fluorescentes
C) Incandescentes

97. Porcentaje de funcionalidad de lámparas

A) 80% al 100%
B) 50% al 79%
C) 0%-49%

98. Alcance en mt^2 de iluminación por lámpara

A) Una lámpara por $4m^2$
B) Una lámpara por $6m^2$
C) Una lámpara por $8m^2$

99. Tipo de pintura en las paredes

A) Agua
B) Vinílica
C) Aceite/papel tapiz

100. Color de pintura en las paredes

A) Azul claro
B) Blanco
C) Otro color

4.6. Concentrado de Información

En este cuestionario puede observarse que ninguna pregunta es abierta; está planteado de esta manera para mantener un enfoque imparcial del auditor. Así también, se observa que se emplearon dos métodos de recolección de datos, una es por incisos y otra por selección múltiple de alternativas. Para poder concentrar la información es necesario definir la puntuación de cada pregunta.

En el método por incisos todas las preguntas tienen tres respuestas, por lo tanto el (A) corresponde a 3 puntos, el (B) 2 puntos, y el (C) 1 punto

1. Las licencias de *software* instaladas en los equipos son:
   A) Privadas/gratuitas
   B) De pruebas
   c) Craqueadas

En método por selección múltiple de alternativas, se sugiere aplicar una regla básica de tres elementos, estipulando como valor máximo el 3.
Por ejemplo para obtener (7 * 3) / 9 = 2.3 puntos; empleando la siguiente fórmula:

*(núm. opciones seleccionadas * 3) / núm. opciones totales = PUNTOS*

5. Los Recursos de *software* instalados para funciones básicas son:

☐ Procesador de texto,	☐ Editor de folletos,
☐ Hoja de cálculo,	☐ Editor de tutoriales,
☐ Base de datos,	☐ Navegadores,
☐ Editor de presentaciones	☐ Buscadores
☐ Editor de videos,	

Otra forma, sería una escala de medición, pero no es recomendable por dos razones; primero porque el número de respuestas no es igual en cada pregunta y segundo porque la división de opciones en respuestas impares podría causar desacuerdos.

En este caso no hay ningún problema, porque el número de respuestas permite una división equitativa:

☑ 7, 8, 9..... 3ptos.
☑ 4, 5, 6..... 2 ptos.
☑ 1, 2, 3..... 1 pto.

Pero, en los siguientes casos, la división ocurre de distintas maneras, y los resultados finales serían diferentes en cada una.

☑ 6,7 ..... 3ptos.
☑ 4,5 ..... 2 ptos.
☑ 1,2,3 ..... 1 pto.

☑ 6,7 .. 3ptos.
☑ 3, 4, 5 ... 2 ptos.
☑ 1,2, ... 1 pto.

Es por ello, que se sugiere emplear la primera fórmula.

A continuación se presenta tablas que incluye las preguntas, las respuestas y los puntos obtenidos por incisos u opciones de la sección de Tecnología *(ver Fig. 55, 56 y 57)*.

Figura 55. Tecnología [Software]

No.	Descripción	Inciso seleccionado	Opciones seleccionadas	Puntos Obtenidos
Tecnología (Software, Hardware y Redes)				
Software:				
1	Las licencias de *software* instaladas en los equipos son:	A		3
2	Tipo de sistemas operativos empleado para servidores	B		2
3	Sistemas operativos instalados en los equipos. **(3 opciones)**		2	2
4	Recursos de *software* instalados para funciones. **(9 opciones)**		6	2
5	Recursos de *software* instalados para funciones de limpieza del sistema. **(6 opciones)**		5	2.5
6	Recursos de *software* instalados para la administración del Sistema. **(4 opciones)**		4	3
7	Recursos de *software* instalados para la administración de base de datos	C		1
8	Periodicidad con que se realiza un análisis de virus	A		3
9	Periodicidad con que se realiza el cambio de contraseñas	B		2
10	Mecanismo se emplea para el control de acceso lógico	B		2
11	El control de equipo por usuario:	A		3
12	Periodicidad con que se respaldan los datos	B		2
13	Estrategias de seguridad empleadas en el control de transacciones. **(5 opciones)**		3	1.8
14	Protocolo de recuperación de datos **(3 opciones)**		2	2
15	Protección de datos de carácter personal, considerados como nivel ALTO. **(6 opciones)**		4	2
16	Protección de datos de carácter personal, considerados como nivel MEDIO. **(4 opciones)**		3	2.25
17	Protección de datos de carácter personal, considerados como nivel BAJO **(4 opciones)**		1	0.75

18	Periodicidad en que se aplican los protocolos de seguridad en páginas Web.	C		1
19	El protocolo de seguridad en páginas Web, incluye la depuración: **(4 opciones)**		3	2.25
20	Qué estrategias de seguridad se emplean para la protección de los datos en la página WEB **(3 opciones)**		2	2
21	Monitoreo y supervisión de actividades en la Web, que realizan los usuarios en los equipos, es a través de:	A		3
			Subtotal	**44.55**

Fuente [elaboración propia]

Figura 56. Tecnología [Hardware]

Hardware:				
No.	**Descripción**	**Inciso seleccionado**	**Opciones seleccionadas**	**Puntaje**
22	Capacidad RAM, promedio de los equipos	B		2
23	Capacidad de Disco Duro, promedio de los equipos	B		2
24	Componentes que incluyen el promedio de los equipos: **(4 opciones)**		3	2.25
25	Dispositivos de almacenamiento que incluyen el promedio de los equipos: **(5 opciones)**		3	1.8
26	Dispositivo de almacenamiento para hacer los respaldos de las BD	B		2
27	Medidas de seguridad se aplican a los dispositivos USB que ingresan a las computadoras. **(3 opciones)**		2	2
28	Recursos de *hardware* se le realiza mantenimiento preventivo. **(4 opciones)**		4	3
29	Periodicidad con que se realiza el mantenimiento preventivo del *hardware*	B		2
30	Protocolo ambiental para el tratamiento de los residuos de cómputo.	C		1

31	Protocolo para la destrucción de los dispositivos de almacenamiento y la información contenida.	B		2
			Subtotal	**20.05**

Fuente [elaboración propia]

Figura 57. Tecnología [Redes]

Redes:				
No.	**Descripción**	**Inciso seleccionado**	**Opciones seleccionadas**	**Puntos Obtenidos**
32	Tipo de conexión en la red	A		3
33	La asignación de las IP a los equipos de red es	A		3
34	Controles de acceso para la conexión a internet :	A		3
35	Asignación de la IP para los servidores:	A		3
36	Material de las vías de acceso	C		1
37	Tipo de encriptación para la red inalámbrica	B		2
38	Protocolo empleado para enviar datos a tu base de datos vía inalámbrico	B		2
			Subtotal	**17**

Fuente [elaboración propia]

De la misma manera, se presenta las siguientes tablas que incluyen las preguntas, las respuestas y los puntos obtenidos en la sección de Gestión Administrativa *(ver Fig. 58 y 59)*.

Figura 58. Gestión Administrativa [Recurso Humano]

No.	**Descripción**	**Inciso seleccionado**	**Opciones seleccionadas**	**Puntos Obtenidos**
Gestión Administrativa (Recurso Humano y Procedimientos)				
Recurso Humano:				
39	Personal que integra el área de sistemas: **(6 opciones)**		3	1.5
40	Perfil académico del responsable del área de sistemas	B		2

41	Funciones del el área de sistemas. **(8 opciones)**		5	1.88
42	Antigüedad comprobable del responsable en el área de Sistemas	C		1
43	Conocimientos comprobables del responsable en el área de Sistemas. **(4 opciones)**		2	1.5
44	Documentos probatorios de conocimientos del responsable en el área de Sistemas. **(4 opciones)**		3	2.25
45	Habilidades del responsable en el área de Sistemas. **(4 opciones)**		1	0.75
46	Personal que realiza el servicio de mantenimiento preventivo / correctivo.	A		3
47	Personal que realiza los respaldos de las BD	B		2
48	Habilidades se evalúan en los analista/programadores. **(6 opciones)**		5	2.5
49	Para medir el desempeño laboral de los analista /programadores. **(4 opciones)**		3	2.25
			Subtotal	**20.63**

Fuente [elaboración propia]

Figura 59. Gestión Administrativa [Procedimientos]

No.	Descripción	Inciso seleccionado	Opciones seleccionadas	Puntos Obtenidos
Procedimientos:				
50	Documentos existentes para el control administrativo en el área de Sistemas. **(6 opciones)**		5	2.5
51	Documentos para el control operativo en el área de Sistemas.**(4 opciones)**		3	2.25
52	Documentos relacionados al control administrativo y operativo. **(4 opciones)**		2	1.5
53	Estrategias de evaluación de los procedimientos internos del área:	B		2
54	El Control de contraseñas se actualiza:	C		1
55	El Control de "Equipo", presenta los siguientes datos. **(4 opciones)**		3	2.25
56	El Control de "Usuario", presenta los siguientes datos. **(4 opciones)**		1	0.75
57	Control para el uso de dispositivos USB, memorias y discos portables		4	2

	que ingresan en los equipos.(**6 opciones)**			
58	Control de los respaldos de las Bases de Datos (Backup). **(4 opciones)**		3	2.25
59	Ubicación de los respaldos de seguridad	B		2
60	Datos del Inventario de Cómputo.**(6 opciones)**		5	2.5
61	Datos del Inventario de *software*. **(6 opciones)**		4	2
62	Datos del Inventario de *hardware*.**(7 opciones)**		6	2.57
63	Lineamientos de la Adquisición de *software*.**(4 opciones)**		2	1.5
64	Elección del proveedor. **(6 opciones)**		4	2
65	Documentos relacionados al diseño y desarrollo de Programas. **(5 opciones)**		5	3
66	Programas de Aplicación WEB. **(6 opciones)**		4	2
67	Planes en casos de una emergencia. **(3 opciones)**		3	3
68	Acciones de prevención ante una amenaza. **(3 opciones)**		2	2
69	Acciones con los Planes de Riesgo, Contingencia y/o Continuidad. **(3 opciones)**		3	3
70	Riesgos que se incluyen en los planes **(12 opciones).**		8	2
71	Elementos de Plan de Riesgo. **(8 opciones)**		6	2.25
72	Elementos del Plan de Contingencia. **(4 opciones)**		4	3
73	Elementos del Plan de Continuidad. **(5 opciones)**		5	3
			Subtotal	**52.32**

Fuente [elaboración propia]

Finalmente se presentan las tablas que incluyen las preguntas, respuestas y los puntos obtenidos en la sección de Recursos Físicos *(ver Fig. 60 y 61)*.

Figura 60. Recursos Físicos [Infraestructura]

No.	Descripción	Inciso seleccionado	Opciones seleccionadas	Puntos Obtenidos
RECURSOS FÍSICOS (Infraestructura y Materiales)				
Infraestructura:				
74	Área física (mts$^{2)}$ por persona	B		2
75	Material de construcción del área de sistemas	B		2
76	El área de sistemas está ubicada en una zona, que evita los riesgos. **(6 opciones)**		4	2
77	Medidas de prevención en caso de un incendio. **(8 opciones)**		6	2.25
78	Medidas de prevención en caso de un desastre natural. **(6 opciones)**		4	2
79	Medidas de prevención en caso de vandalismo y actividades ilícitas (5 **opciones)**		2	1.2
80	Relación de contactos por computadoras	B		2
81	Tipo de instalación de los contactos: (3 **opc.)**		1	1
82	Porcentaje de funcionalidad de los contactos.	A		3
83	Características del cable: **(3 opciones)**		2	2
84	Mecanismos de prevención por sobrecarga de voltaje:	C		1
85	Fuente de corriente eléctrica para el área de sistemas. **(4 opciones)**		2	1.5
86	El mantenimiento preventivo se realiza en: **(4 opciones)**		2	1.5
87	Otros espacios para el servicio del área: **(4 opciones)**		2	1.5
			Subtotal	**24.95**

Fuente [elaboración propia]

Figura 61. Recursos físicos [Materiales]

No.	Descripción	Inciso seleccionado	Opciones seleccionadas	Puntos Obtenidos
Materiales:				
88	Tipo de ventilación en el área de sistema	A		3
89	Cantidad de BTU por metro^2 y por Zona	B		2
90	Requisitos del Aire Acondicionado **(4 opciones)**		2	1.5

91	Tipo de Extintores en el área de Sistemas	A		3
92	Características del Extintor. **(5 opciones)**		3	1.8
93	Tipo de mesas y sillas disponibles para el equipo de cómputo	C		1
94	Material de fabricación de mesas	C		1
95	Material de fabricación de sillas. **(3 opciones)**		2	2
96	Tipo de fabricación de lámparas	B		2
97	Porcentaje de Funcionalidad de lámparas	B		2
98	Alcance en m2 de iluminación por lámpara	B		2
99	Tipo de pintura en las paredes	C		1
100	Color de pintura en las paredes	C		1
			Subtotal	**23.3**

Fuente [Elaboración Propia]

4.7. Resultados

A partir del ejemplo anterior, a continuación se presenta la puntuación obtenida por cada sub-área *(ver Fig. 62)*:

Figura 62. Concentrado de Resultados

Tecnología			
Sub-área	Núm. Preguntas	Puntuación máxima que se puede obtener	Puntuación obtenida
Software	21	63	*44.55*
Hardware	10	30	*20.05*
Redes	7	21	*17.00*
Total >>	38	114	***81.6 puntos***
Gestión Administrativa			
Sub-área	Núm. Preguntas	Puntuación máxima que se puede obtener	Puntuación obtenida
Recurso Humano	11	33	
Procedimientos	24	72	*52.32*
Total >>	35	105	***72.95 puntos***
Recursos Físicos			
Sub-área	Núm. Preguntas	Puntuación máxima que se puede obtener	Puntuación obtenida
Infraestructura	14	42	*24.95*
Materiales	13	39	*23.30*
Total>>	27	81	***48.25 puntos***

Fuente [Elaboración propia]

CAPÍTULO V

METODOLOGÍA PARA DISEÑAR *SOFTWARE* DE AUDITORÍA EN INFORMÁTICA

Metodología de Trabajo

Cuestionario Electrónico

Programa Diagnóstico Automatizado

Medición de Intervalos

Medición Ordinal

Dictamen

Sugerencias

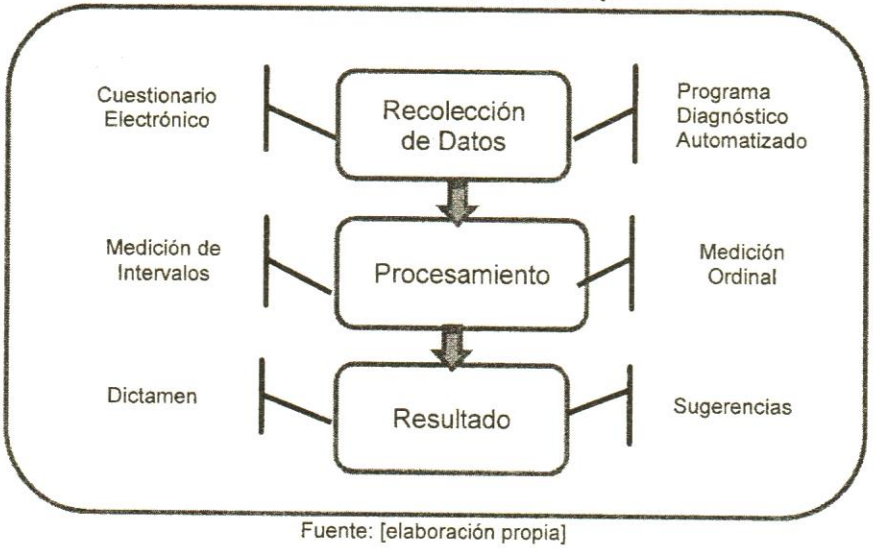
5.1. Metodología de Trabajo

Este capítulo ofrece una opción de Auditoría en Sistemas Computacionales y/o Informática asistida por la tecnología; que consiste en el diseño y desarrollo de un Sistema Experto que realice una evaluación, un Dictamen y genere sugerencias.

Con esto, las personas directamente beneficiadas son los auditores en el área, asimismo, puede ser empleado por administradores de negocios como un mecanismo de autoevaluación, y por docentes o estudiantes interesados en la temática aquí abordada, para fortalecer el contenido académico de cátedras relacionadas.

La metodología empleada incluye tres etapas: la primera extrae los datos que se encuentran en los reportes diagnósticos emitidos por los programas comerciales y en los cuestionarios electrónicos; la segunda crea una estructura para depositar los datos extraídos, con parámetros de medición y criterios de evaluación, y la última genera el dictamen y las sugerencias correspondientes *(ver Fig.63)*.

Figura 63. Metodología de Trabajo



Fuente: [elaboración propia]

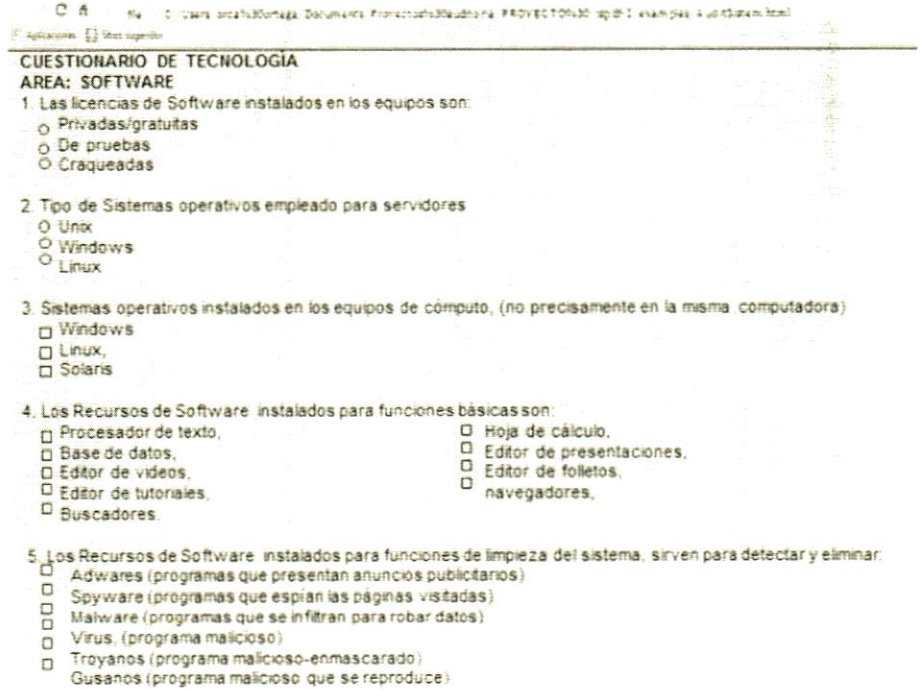
5.2. Recolección de Datos

5.2.1. Cuestionario electrónico

Es un instrumento automatizado que permite obtener información sobre aspectos administrativos en las áreas de Tecnología, Recursos Humanos, Gestión, Infraestructura y Recursos Materiales, en relación al procesamiento de datos y todo lo que le rodea; para conocer las características físicas y lógicas de los equipos, medidas de control, nivel de seguridad, manejo del personal, aplicación de normas, calidad del mobiliario y muchas otras cosas más.

Se presentan dos Cuestionarios programados en HTML y JAVA, con la finalidad de convertir la información en datos procesables; a partir de las preguntas del cuestionario planteadas en el *Capítulo IV, tema 4.5.1, (ver Fig. 64 y 65).*

Figura 64. Cuestionario en HTML



CUESTIONARIO DE TECNOLOGÍA
AREA: SOFTWARE

1. Las licencias de Software instalados en los equipos son:
   - ○ Privadas/gratuitas
   - ○ De pruebas
   - ○ Craqueadas

2. Tipo de Sistemas operativos empleado para servidores
   - ○ Unix
   - ○ Windows
   - ○ Linux

3. Sistemas operativos instalados en los equipos de cómputo, (no precisamente en la misma computadora)
   - □ Windows
   - □ Linux,
   - □ Solaris

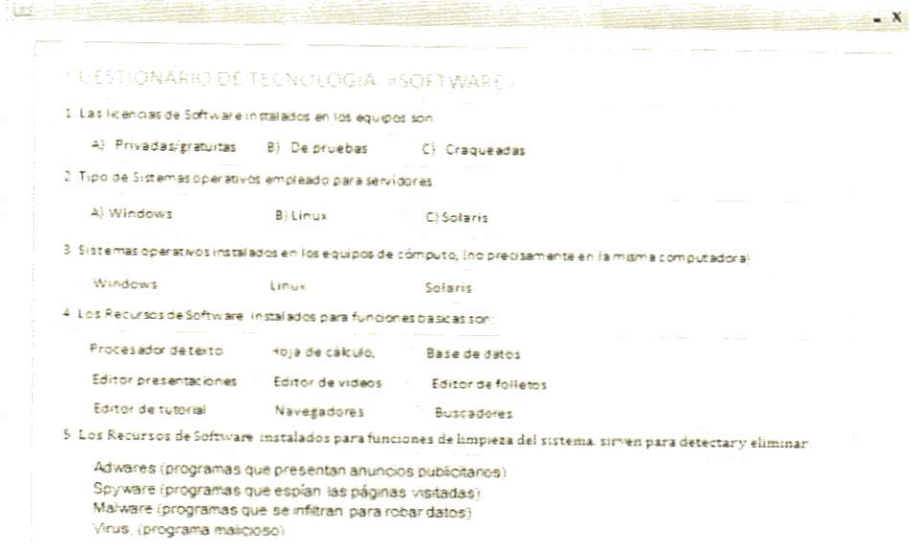
4. Los Recursos de Software instalados para funciones básicas son:
   - □ Procesador de texto,
   - □ Base de datos,
   - □ Editor de videos,
   - □ Editor de tutoriales,
   - □ Buscadores.
   - □ Hoja de cálculo,
   - □ Editor de presentaciones,
   - □ Editor de folletos,
   - □ navegadores,

5. Los Recursos de Software instalados para funciones de limpieza del sistema, sirven para detectar y eliminar:
   - □ Adwares (programas que presentan anuncios publicitarios)
   - □ Spyware (programas que espían las páginas visitadas)
   - □ Malware (programas que se infiltran para robar datos)
   - □ Virus, (programa malicioso)
   - □ Troyanos (programa malicioso-enmascarado)
   - Gusanos (programa malicioso que se reproduce)

Fuente: [Elaboración Propia]

Los círculos representan los incisos A), B) o C) y solo se puede escoger una de las tres opciones, mientras que los cuadrados pueden seleccionarse más de una alternativa.

Figura 65. Cuestionario en Java



Fuente: [Elaboración Propia]

Se puede apreciar que en la imagen anterior unas respuestas tienen incisos y otras no, esto se debe a que en las preguntas 1 y 2, solo se puede seleccionar una opción, a diferencia de las preguntas 3,4, y 5, que pueden seleccionarse más de una.

Aunque ya se mencionó en el capítulo anterior, conviene recordar que el inciso A) tiene un valor de 3 puntos, el B) = 2 puntos y el C) = 1 punto. Las preguntas que tienen selección múltiple, mientras más opciones se elijan, mayor será la puntuación obtenida. Siendo el máximo 3 puntos.

Se recomienda que el Cuestionario sea respondido por el auditor y no por el administrador del área; debido a que se alterarían los resultados y no reflejarían la situación real. Asimismo, se sugiere que se responda en un lugar privado y tranquilo, en base a la visita y entrevista realizada al personal; es válido solicitar la evidencia necesaria para asegurar la fidelidad de las respuestas.

Después de crear las interfaces, se trabaja con la declaración de variables.

Por ejemplo, *TSx* es una variable que representa el *área de Tecnología y Software junto al número de la pregunta*, con el objetivo de almacenar la puntuación obtenida en cada respuesta.

La tabla siguiente *(ver Fig. 66)* recopila las preguntas que solamente tienen tres alternativas como respuestas y le asigna el valor a cada una.

Figura 66. Variables de respuestas con tres incisos

No.	Preguntas	A	B	C	Variable
1	Licencias de *Software*	3	2	1	TS1
2	Sistema Operativo (servidores)	3	2	1	TS2
7	Administración de Base de Datos	3	2	1	TS7
8	Análisis de virus	3	2	1	TS8
9	Cambio de contraseñas	3	2	1	TS9
10	Acceso Lógico	3	2	1	TS10
11	Control de equipo por usuario	3	2	1	TS11
12	Periodo de respaldo de datos	3	2	1	TS12
18	Protocolos de seguridad	3	2	1	TS18
21	Monitoreo actividades WEB	3	2	1	TS21

Fuente [Elaboración propia]

Para las preguntas de múltiples opciones, se crea otra tabla diferente *(ver Fig. 67)*, que contiene las preguntas y la puntuación en relación al número de opciones seleccionadas.

Pregunta 3. Sistemas Operativos
Pregunta 4. Recursos de *Software*
Pregunta 5. Limpieza del Sistema
Pregunta 6. Administración del Sistema
Pregunta 13. Control de Transacciones
Pregunta 14. Protocolo de Recuperación
Pregunta 15. Protección de Datos (nivel alto)
Pregunta 16. Protección de Datos (nivel medio)
Pregunta 17. Protección de Datos (nivel bajo)
Pregunta 19. Protocolo de Seguridad
Pregunta 20. Protección de Datos en la *WEB*

Figura 67. Variables de respuestas múltiples

No. Pg	R1	R2	R3	R4	R5	R6	R7	R8	R9	Var
3	1	1	1							TS3
4	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	TS4
5	0.5	0.5	0.5	0.5	0.5	0.5				TS5
6	0.75	0.75	0.75	0.75						TS6
13	0.6	0.6	0.6	0.6	0.6					TS13
14	1	1	1							TS14
15	0.5	0.5	0.5	0.5	0.5	0.5				TS15
16	0.75	0.75	0.75	0.75						TS16
17	0.75	0.75	0.75	0.75						TS17
19	0.75	0.75	0.75	0.75						TS19
20	1	1	1							TS20

Fuente [Elaboración propia].

Al finalizar, se obtiene un total con la suma de todas las variables inicializadas: *Stotal:= TS1+TS2+TS3 +... + TS19+TS20+TS21.*

Este ejercicio solo abarca 21 preguntas pertenecientes al área de *software*, pero la finalidad es repetir el procedimiento en las áreas restantes hasta cubrir el total de las 100 preguntas del Cuestionario *(ver Fig. 68).*

Figura 68. Número de preguntas por área

Tecnología	Número Preguntas	Gestión Administrativa	Número Preguntas	Recursos Físicos	Número Preguntas
Software	***21***	Recursos Humanos	***11***	Infraestructura	***14***
Hardware	***10***	Procedi-mientos	***24***	Materiales	***13***
Redes	***7***				
TOTAL >>	**38**		***35***		***27***

Fuente [Elaboración propia].

Otro dato importante, es identificar la máxima puntuación que se obtiene de cada área, para lograrlo es necesario que todas las preguntas seleccionen como respuesta el inciso A) o todas las alternativas posibles en la categoría de opción múltiple *(ver Fig. 69).* La suma de los totales debe de presentar 300 puntos repartidos de la siguiente manera:

TTEC= Stotal+Htotal+Rtotal = (63+30+21) = 114
TGA= RHtotal+Ptotal = (33+ 72) =105
TRF= Mattotal+Inftotal = (42 + 39) = 81
TOTAL= TTEC + TGA + TRF = (114 + 105 + 81)=300 puntos

Figura 69. Máxima puntuación por área

Tecnología	Máxima puntuación	Gestión Administrativa	Máxima puntuación	Recursos Físicos	Máxima puntuación
Software	***63***	Recursos Humanos	***33***	Infraestructura	***42***
Hardware	***30***	Procedimientos	***72***	Materiales	***39***
Redes	***21***				
TOTAL >>	**114**		***105***		***81***

Fuente [Elaboración propia].

5.2.2. Diagnóstico Automatizado

¿Por qué emplear un Programa de Diagnóstico? y ¿Por qué programar un programa?, en el Capítulo III se describe el funcionamiento de 15 programas que trabajan en diferentes plataformas, en forma local o remota, con distintas funciones pero con el mismo objetivo: generar un reporte en las áreas de *software, hardware*, redes y comunicaciones, base de datos y ambiente *WEB*, según su especialidad; los reportes pueden ser emitidos en formatos *html, xls, pdf* u otros y presentan información de seriales, nombres, descripciones, componentes, características, estadísticas, etc., de cada equipo.

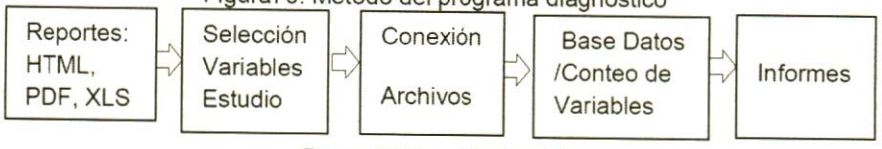
Ahora bien, debe realizarse esta operación el número de veces que represente el número de máquinas a revisar, por lo tanto, los listados se multiplican y se convertirán en muchas horas de trabajo; el alcance del proyecto de auditoría juega un papel muy importante al momento de elegir el número de atributos de estudio en cada reporte, para concentrar, contabilizar y analizar correctamente la información.

La idea de generar un programa a partir de un Programa, representa la oportunidad de automatizar un proceso manual, que brinde un informe más que un diagnóstico, en menor tiempo y con menor esfuerzo, beneficiando directamente el desempeño del auditor.

En base a lo anterior, se propone crear una aplicación que utilice como datos de entrada los reportes de los programas diagnósticos, seleccione las variables de estudio según el alcance del proyecto, realice una conexión del archivo *html, pdf o xls,* con un lenguaje de programación, diseñe base de datos y cuando la información ya se encuentra en un medio

estructurado, registre el número de incidencias, realice comparaciones y finalmente emita un informe más robusto y de mayor utilidad al auditor. *(Ver Fig.70)*.

Figura70. Método del programa diagnóstico



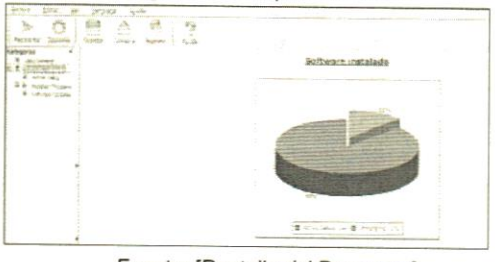
Fuente [Elaboración Propia]

Caso Práctico

Para obtener un informe que presente el estado actual de las computadoras sobre el licenciamiento de los programas instalados en cada una, se plantea tomar como referencia el programa *WinAudit* y se observarán los pasos descritos.

a) ***Reportes en HTML, PDF o XLS***. Para obtener el reporte primero se selecciona las categorías "*software instalado*" y "vista general" *(ver Fig. 71)*.

Figura 71. Reportes HTML

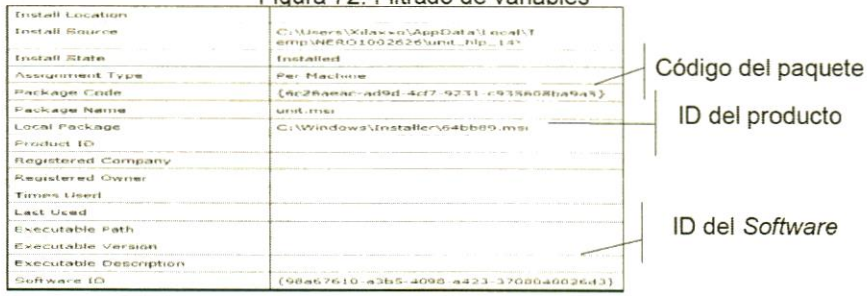


Fuente: [Pantalla del Programa]

b) ***Selección de variables***. Las pantallas de *software* instalados presentan información sobre las características de cada uno.

Para poder realizar un análisis es necesario filtrar los siguientes atributos *Package Code, Product ID y Software ID* que significa código del paquete, identificación del producto y del *software (ver Fig. 72)* :

Figura 72. Filtrado de variables



Install Location	
Install Source	C:\Users\Xdaxco\AppData\Local\Temp\NERO1002626\unit_hlp_14\
Install State	Installed
Assignment Type	Per Machine
Package Code	{8c28aeac-ad9d-4cf7-9231-c935608ba9a8}
Package Name	unit.msi
Local Package	C:\Windows\Installer\64bb89.msi
Product ID	
Registered Company	
Registered Owner	
Times Used	
Last Used	
Executable Path	
Executable Version	
Executable Description	
Software ID	{98a67610-a3b5-4098-a423-370804002643}

Fuente: [Pantalla del Programa]

c) ***Conexión de archivos***. La librería *JFileChooser* del lenguaje *NetBeans;* obtiene el archivo del reporte y la ruta que genera *WinAudit (ver Fig. 73)*.

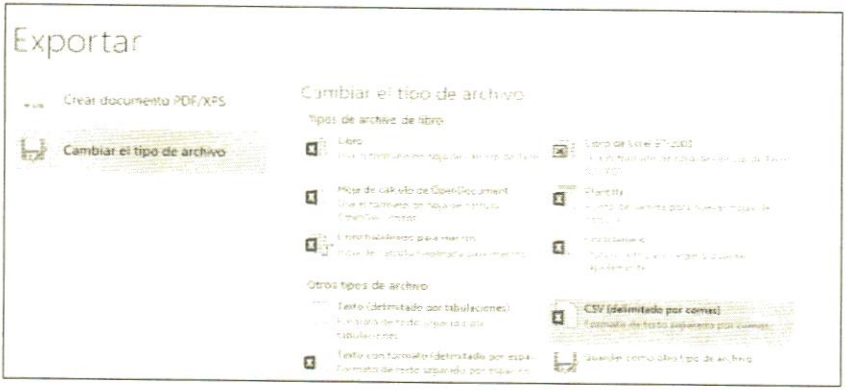
Figura 73. Conexión por archivos

```
private void jFileChooser2ActionPerformed(java.awt.event.ActionEvent evt) {
  JFileChooser selectorArchivo=(JFileChooser)evt.getSource();
    String comando=evt.getActionCommand();
    if(comando.equals(JFileChooser.APPROVE_SELECTION))
    {
      try {
          File archivo=selectorArchivo.getSelectedFile();
          ruta = archivo.getPath();
        System.out.print(ruta);
           jDialog1.setVisible(false);
           truncar_table();
           seleccion1(ruta);
            seleccion2(ruta);
          seleccion3(ruta);
              puntos_s();
               truncar_table();

      } catch (IOException ex) {
          Logger.getLogger(auditar_doc.class.getName()).log(Level.SEVERE, null, ex);
      }
```

Fuente: [Fragmento de Código]

Otra alternativa para realizar la conexión puede ser, copiar el archivo *html* de *WinAudit* a una hoja *xls*; convertir la hoja de cálculo a formato *.cvs* separado por comas *(ver Fig. 74)*, y finalmente importar el archivo *.csv* a *phpMyadmin* dentro de una base de datos.

Figura 74. Conexión por base de datos



Fuente: [Pantalla del Programa]

d) ***Base de datos y conteo de variables.*** Se presenta un fragmento del programa que contabiliza las incidencias del código del paquete (cont_pc), que presenta el reporte. Las variables de estudio se declaran en 0 al inicio del programa (cont_pc=0) y se van incrementando en cada ciclo (cont_pc++), *(ver Fig. 75).*

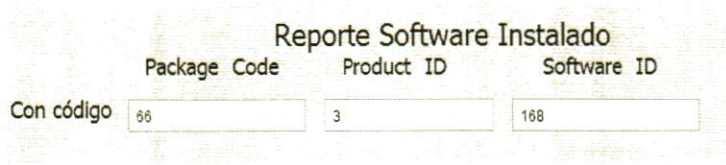
Figura 75. Conteo de variables

```
@SuppressWarnings("unchecked")
public static int cont_pi=0, cont_si=0, cont_pc=0;
   public static void seleccion1(String ruta) throws IOException{
       cont_pc=0;

 String cadena=null;
     BufferedReader br = new BufferedReader(new InputStreamReader(System.in));
 System.out.print("[illegible]");
 cadena ="[illegible]";
    try{
         conexion2 cnx=new conexion2();
             cnx.cnx();
               BufferedReader bufferedReader = new BufferedReader(new FileReader(ruta));
                    String line = "";
                    String str1=null;
                    while((line = bufferedReader.readLine())!=null)
                    {

                            if(line.indexOf(cadena)!= -1){
                                cont_pc++;
                               str1="[illegible]"+line+"[illegible]";
                               cnx.stmt.executeUpdate(str1);
                                System.out.println(line);
                            }
                    }
         cnx.getConexion();

}catch(Exception e){ e.printStackTrace();}
}
```

Fuente: [Fragmento de Código]

e) ***Informe.*** Consiste en diseñar una pantalla que presente los resultados almacenados en una estructura ordenada que refleje el registro de incidencias *(ver Fig. 76)*.

Figura 76. Registro de incidencias



Fuente: [Pantalla del Programa]

5.3. Procesamiento

5.3.1. Medición de intervalos y Medición Ordinal

La Medición de intervalos se emplea ante la necesidad de agrupar los datos, definiendo un dato de inicio y otro final, donde la clase con la puntuación más alta representa mayor control y calidad, y la más baja indica lo contrario. En la Medición Ordinal o Escala *Likert* se busca evaluar cada clase; generalmente representada por 5 criterios, donde el 5 indica "excelente", el 4 "bien", el 3 "regular", el 2 "mal" y 1 "deficiente"; pero en esta propuesta solo se emplean tres de ellos: "Excelente, Regular y Deficiente".

Por ejemplo, para determinar la longitud del intervalo se toma la puntuación máxima por sub-área, que se obtiene multiplicando el número de preguntas por 3 que representa los puntos máximos por alcanzar en cada una y luego se divide entre 3 que indican los estados ordinales.

Para visualizar los datos seleccionaremos *Software* del área de Tecnología, la cual contiene 21 preguntas que al multiplicarse por los 3 puntos máximos a obtener, el resultado es 63 puntos, los cuales se dividen entre los 3 criterios que se representan como: "excelente, regular y deficiente". En términos de fórmulas, quedaría de la siguiente manera:

Rango= ((núm. Preguntas) X (3 puntos)) / (3 criterios)

A continuación se presentan tablas con los intervalos y escala de cada área y su correspondiente sub-área *(ver Fig. 77)*.

Figura 77. Intervalos del Cuestionario Electrónico

Tecnología (Software, Hardware y Redes)				
Sub-área	Núm. Preguntas	Puntuación máxima	Intervalos	Escala
Software	21	63	43-63 22-42 0-21	Excelente Regular Deficiente
Hardware	10	30	21-30 11-20 0-10	Excelente Regular Deficiente
Redes	7	21	16-23 9-15 0-8	Excelente Regular Deficiente
Gestión Administrativa				
Sub-área	Núm. Preguntas	Puntuación máxima	Intervalos	Escala
Recurso Humano	11	33	23-33 12-22 0-11	Excelente Regular Deficiente
Procedimientos	24	72	49-72 25-48 0-24	Excelente Regular Deficiente
Recursos Físicos				
Sub-área	Núm. Preguntas	Puntuación máxima	Intervalos	Escala
Infraestructura	14	42	29-42 15-28 0-14	Excelente Regular Deficiente
Material	13	39	27-39 14-26 0-13	Excelente Regular Deficiente

Fuente: [Elaboración Propia]

Los intervalos están sujetos al diseño expreso de este Cuestionario, cualquier modificación al número de preguntas o al valor que se le asigne a cada respuesta, ocasiona alteraciones. Sin embargo esto no quiere decir, que el auditor no pueda emplear otros reactivos, solo se recomienda asegurarse que se ajuste a la metodología propuesta.

Una vez definidos los niveles en este instrumento de recolección de datos, se procede con el *Diagnóstico Automatizado*, que observa una

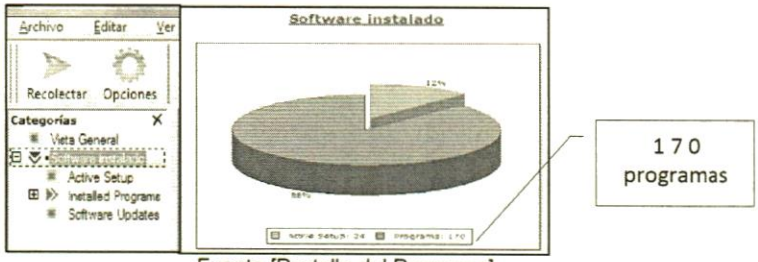
mecánica diferente, porque los valores incluidos en los intervalos se sujetan a la información de cada computadora.

Para explicarlo con mayor detalle, se retoma el caso de estudio de *WinAudit* del tema 5.1.2., que registra el código del paquete, id del producto e id del *software* de los programas instalados en un equipo; en esta ocasión para obtener el rango de cada intervalo es necesario conocer el número total de programas y dividirlo entre los tres estados ordinales, esta acción se repite según el número de atributos seleccionados. En términos de fórmulas, se aprecia de la siguiente manera:

Rango = (Número Total Programas / Número de estados)

Para visualizar el procedimiento anterior, se presenta el número de programas instalados en un equipo y los intervalos correspondientes *(ver Fig. 78 y 79)*,

Figura 78. Número de programas instalados



Fuente [Pantalla del Programa]

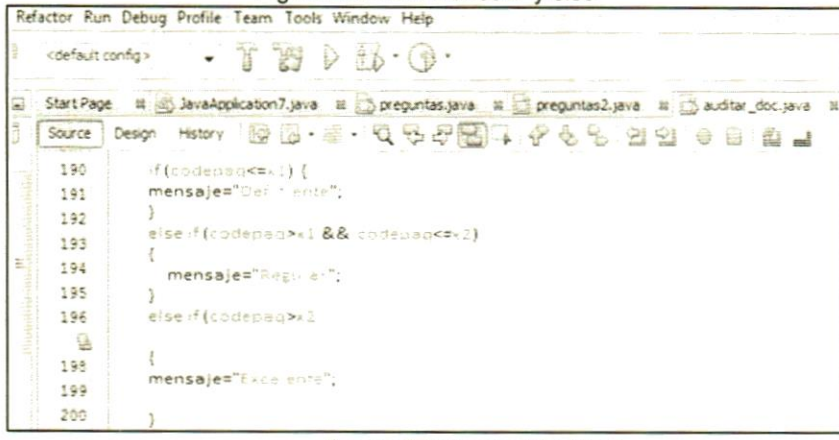
Figura 79. Intervalos del Programa Diagnóstico Automatizado

Atributos	Intervalos	Escala
Código del paquete	115 – 170 58 - 114 0 – 57	Excelente Regular Deficiente
Id del producto	115 – 170 58 - 114 0 – 57	Excelente Regular Deficiente
Id del *software*	115 – 170 58 - 114 0 – 57	Excelente Regular Deficiente

Fuente [Elaboración Propia]

Las condiciones *"if"* y *"else"* tienen el mismo intervalo, porque se refieren al mismo objeto *(ver Fig. 80)*.

Figura 80. Condiciones *if* y *else*



Fuente: [Fragmento del código]

5.4. Resultados

La metodología contempla una etapa de resultados que presenta el dictamen final y las sugerencias obtenidas en todo el proceso de evaluación; mismos que serán entregados al representante del negocio para la adecuada toma de decisiones en relación a la actualización o adecuación de los controles existentes.

5.4.1. Dictamen

Son los resultados que se clasifican en tres estados, los cuales son: "excelente, regular y malo" y se aplican al Cuestionario Electrónico y al Programa Diagnóstico Automatizado.

5.4.1.1. Cuestionario electrónico

Para obtener del dictamen parcial de cada sub-área *(ver Fig.*81), se presenta la puntuación obtenida de la aplicación del cuestionario electrónico en una ambiente real y se compara con los intervalos definidos en la figura 77. "Intervalos del Cuestionarios Electrónico".

Figura 81. Dictamen por Intervalos del Cuestionario [Sub-áreas]

Tecnología (Software, Hardware y Redes):					
Sub-área	Número Preguntas	Puntuación obtenida	Intervalos	Escala	Estado [E,R,D]
Software	21	***44.55***	43-63 22-42 0-21	Excelente Regular Deficiente	***Excelente***
Hardware	10	***20.05***	21-30 11-20 0-10	Excelente Regular Deficiente	***Regular***
Redes	7	***17.00***	16-23 8-15 0-7	Excelente Regular Deficiente	***Excelente***
Gestión Administrativa:					
Sub-área	Número Preguntas	Puntuación obtenida	Escala de puntuación	Escala	Estado [E,R,D]
Recurso Humano	11	***20.63***	23-33 12-22 0-11	Excelente Regular Deficiente	***Regular***
Procedi-mientos	24	***52.32***	49-72 25-48 0-24	Excelente Regular Deficiente	***Excelente***
Recursos Físicos					
Sub-área	Número Preguntas	Puntuación obtenida	Intervalos	Escala	Estado [E,R,D]
Infraes-tructura	14	***24.95***	29-42 15-28 0-14	Excelente Regular Deficiente	***Regular***
Material	13	***23.3***	27-39 14-26 0-13	Excelente Regular Deficiente	***Regular***

Fuente [Elaboración Propia].

El dictamen parcial de las tres áreas, se obtiene al definir nuevamente los intervalos en relación a la máxima puntuación y al número de preguntas, el dictamen final se basa en la comparación del resultado total con los 300 puntos máximos que pueden obtenerse del Cuestionario y que se presenta como dato mayor del intervalo *(ver Fig. 82)*.

Figura 82. Dictamen por Intervalos del Cuestionario [Áreas]

Área:	Número Preguntas	Puntaje obtenido	Intervalo	Escala	Estado [E,R,D]
Tecnología	38	**81.6 puntos**	77-114 39-76 0-38	Excelente Regular Deficiente	***Excelente***
Gestión Administrativa	35	**72.95 puntos**	71-105 36-70 0-35	Excelente Regular Deficiente	***Excelente***
Recursos Físicos	27	**48.25 puntos**	55-81 30-54 0-29	Excelente Regular Deficiente	**Regular**
TOTAL= Tecnología + Gestión Administrativa+ Recursos Físicos		**202.8 puntos**	201-300 101-200 0-100	Excelente Regular Deficiente	***Excelente***

Fuente [Elaboración Propia]

Al terminar el ejercicio, el ***dictamen final*** *del Cuestionario con la técnica de medición de intervalos en relación a una escala establecida es la siguiente:* ***202.8 puntos igual a "Excelente".***

Otra técnica que se puede emplear es la combinación de estados; ésta se puede aplicar en las subáreas o directamente en las áreas. Pero antes, deben considerarse los siguientes casos:

a) Caso 1. Cuando se presenten tres estados diferentes [*Excelente, Regular y Deficiente*],y aunque no se utiliza estadística descriptiva puede recurrirse a la media aritmética, dando como resultado el estado intermedio: "Regular"

b) Caso 2. Cuando se presentan dos estados iguales y uno diferente [*Excelente. Excelente y Regular*], en esta ocasión se puede aplicar la moda y el resultado es el estado con mayor frecuencia: "Excelente".

c) Caso 3. Cuando se presenta dos estados iguales y uno diferente [*Excelente, Excelente, Deficiente*], es parecido al caso anterior pero no se puede aplicar el mismo criterio porque los datos representan extremos contrarios, y se tiene que optar por el estado intermedio: "Regular", como resultado.

d) Caso 4. Cuando solo existen dos estados y éstos son: *Excelente y Regular*, es diferente a todos los casos anteriores, porque no representa puntos extremos y carece de un tercer elemento que defina la balanza,

por lo tanto el resultado podría ser "Excelente" para unos y "Regular" para otros.

Puede observarse que en cada caso, se justifica el resultado con un enfoque diferente. Una forma de mantener una postura íntegra, ecuánime e imparcial, es definir al principio los criterios de evaluación que se deben emplear; por ejemplo para las áreas de este ejercicio se considera el siguiente criterio:

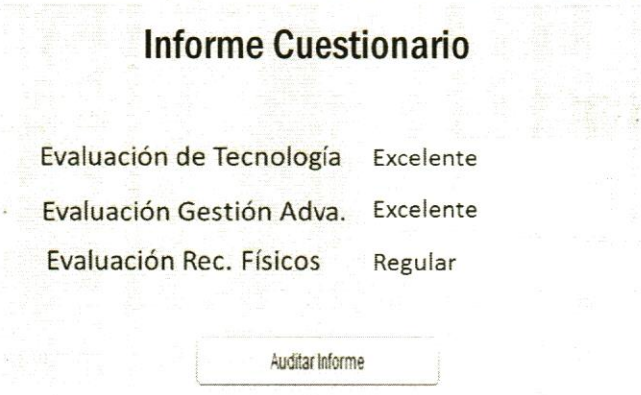
a) El Dictamen es "*Excelente*":
   Si se obtiene en las tres áreas: [E], [E], [E]
   Si se obtiene en dos áreas [E], [E] y en otra [R]

b) El Dictamen es "*Regular*":
   Si se obtiene en las tres áreas: [R], [R], [R]
   Si se obtiene en dos áreas: [R], [R] y en otra [E]

c) El Dictamen es "*Deficiente*" cuando una o más de un área, obtiene como resultado [D].

Después de definir los criterios de evaluación, se presenta la pantalla del programa del Cuestionario Electrónico que contiene el dictamen parcial de Tecnología, Gestión Administrativa y Recursos Físicos; y un botón de "Auditar Informe" *(ver Fig. 83)*.

Figura 83. Dictamen por Combinación de Estados del Cuestionario



Fuente: [Pantalla del Programa]

Al presionar el botón se presenta el **dictamen final,** que en esta ocasión es: ***"Excelente",*** como puede apreciarse es el mismo resultado que se genera con la técnica anterior.

5.4.1.2. Programa diagnóstico automatizado

Para obtener el porcentaje correspondiente de cada *ítem* es necesario considerar que el total de programas instalados corresponden al 100%; por ejemplo, en una aplicación real podría obtenerse un total de 170 programas como universo, de los cuales 66 tienen código del paquete, 3 id del producto y 168 tienen id del *software*. Se observa que la suma de los tres es mayor que 170, esto se debe a que un programa puede cumplir con más de un atributo, como se observa en la tabla siguiente *(ver Fig. 84)*.

Lo idóneo sería que los 170 programas tuvieran el código del paquete, el id del producto y el id del *software*, alcanzando un total de 510 puntos, obtenidos de la multiplicación de 170 por 3. Sin embargo, para su mejor comprensión se estudiará cada atributo en forma individual.

Figura 84. Registro de Incidencias

No	Código del Paquete	Id del Producto	Id del Software
1	✓		✓
2		✓	✓
3	✓		✓
...			
...			
170			
Total	66	3	168

Fuente: [Elaboración Propia]

Si 170 programas equivalen al 100%; entonces a 66 programas, ¿qué porcentaje le corresponde?

Código del Paquete:= (66 *100) / 170 =38.8%

Si 170 programas equivalen al 100%; entonces a 3 programas, ¿qué porcentaje le corresponde?

Id del Producto:= (3 * 100) /170= 1.76%

Si 170 programas equivalen al 100%; entonces a 168 programas, ¿qué porcentaje le corresponde?

Id del *Software*:= (168*100) /170= 98.8%

Si la suma de los tres porcentajes es (38.8+1.76+98.8)=139.36 % y la máxima puntuación posible es 300%, entonces ¿cuál sería el dictamen que corresponde? Para conocer el resultado primero deben definirse los intervalos, como a continuación se describen:

- Si el total es menor que 100 el resultado es "Deficiente"
- Si el total se encuentra entre 100 y 200 el resultado es "Regular"
- Si el total es mayor que 200 el resultado es "Excelente".

Aplicando el criterio descrito, con los datos anteriores, el **dictamen final** es: ***"Regular".*** Porque el total es igual a 139.36% y se encuentra entre 100% y 200%.

Al igual que con el Cuestionario Electrónico, puede aplicarse en este apartado la técnica de combinación de estados, pero primero debe obtenerse el resultado de cada atributo, en relación a su puntuación y escala correspondiente, como se aprecia en la tabla siguiente *(ver Fig. 85)*:

Figura 85. Dictamen por Intervalos del Programa Diagnóstico

Atributos *(Item)*	Puntuación obtenida	Intervalos	Escala	Estado [E,R,D]
Código del Paquete	66	115 – 170 58 - 114 0 – 57	Excelente Regular Deficiente	***Regular***
Id del Producto	3	115 – 170 58 - 114 0 – 57	Excelente Regular Deficiente	***Deficiente***
Id del *software*	168	115 – 170 58 - 114 0 – 57	Excelente Regular Deficiente	***Excelente***

Fuente: [Elaboración Propia].

Después se definen los criterios de evaluación para mantener la postura integra e imparcial del auditor*:*

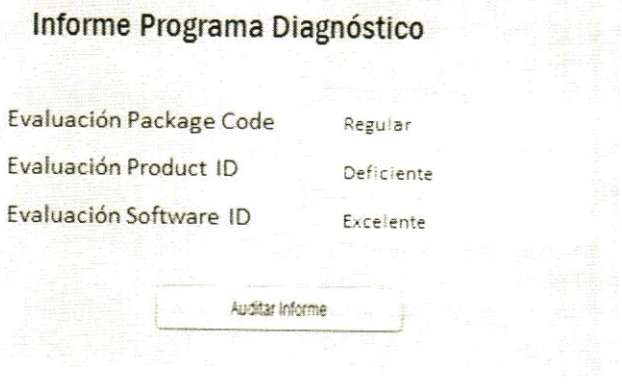
a) El Dictamen es "*Excelente*" :
Si se obtiene en las tres áreas: [E], [E], [E]
Si se obtiene en dos áreas [E], [E] y en otra [R]

b) El Dictamen es "*Regular*" :
Si se obtiene en las tres áreas: [R], [R], [R]
Si se obtiene en dos áreas: [R], [R] y en otra [E]
Si se obtiene en dos áreas: [E], [E] y en otra [D]
Si se obtiene en cada área [E], [R] y [D]

c) El Dictamen es "*Deficiente*" :
Si se obtiene en las tres áreas [D], [D], [D]
Si se obtienen en dos áreas [D], [D] y [E] o [R]
Si se obtiene en una área [D] y en las otras dos [R],[R]

Finalmente, se programa la interfaz que presenta los resultados parciales y el botón de auditar informe, como se aprecia en la siguiente imagen *(ver Fig. 86)*:

Figura 86. Dictamen por Combinación de Estados del Programa Diagnóstico



Fuente: [Pantalla del Programa]

El **dictamen final** obtenido con la combinación de estados "Regular, Deficiente y Excelente" es***: "Regular",*** como se puede apreciar el resultado es el mismo que se genera con la técnica anterior.

5.4.1.3. Dictamen General de Auditoría en informática

Consiste en la presentación de los dictámenes finales obtenidos del **Cuestionario Electrónico** y del **Diagnóstico Automatizado**, con la finalidad de evaluarlos para obtener un dictamen general que represente el estado real de la organización.

Para obtener un resultado ecuánime e imparcial y sobre todo consistente, se mantienen los mismos criterios de evaluación:

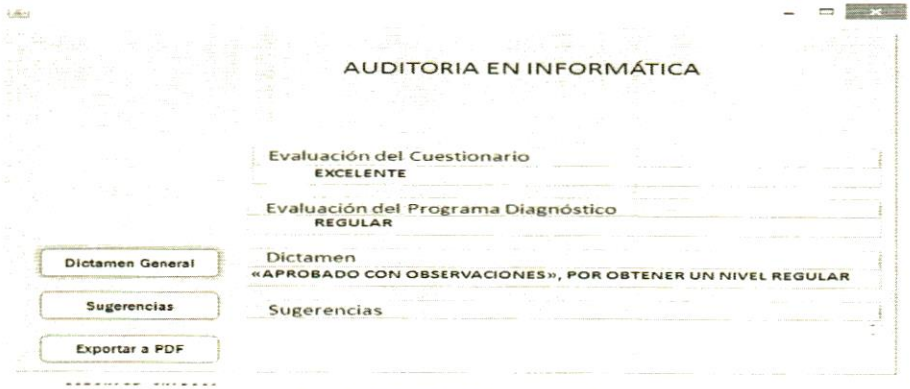
a) El Dictamen es "*Aprobado*":
Si se obtiene en los dos atributos: [E], [E]
Si se obtiene en los dos atributos: [E], [R]

b) El Dictamen es "*Aprobado con observaciones*":
Si se obtiene en los dos atributos: [R], [R],
Si se obtiene en los dos atributos: [D], [E]

c) El Dictamen es "*No Aprobado*":
Si se obtiene en los dos atributos: [D], [D]
Si se obtiene en los dos atributos: [D], [R]

En la interfaz siguiente, se presenta el dictamen final del Cuestionario Electrónico y del Diagnóstico Automatizado, y la opción de Dictamen General *(ver Fig. 87)*:

Figura 87. Dictamen General de Auditoría en Informática



Fuente: [Pantalla del programa]

Como el resultado muestra un estado "Excelente" y otro "Regular", el dictamen General de la Auditoría es ***"Aprobado con Observaciones".***

5.4.2. Sugerencias

Son las recomendaciones que se otorgan al administrador del negocio, en base a la evaluación realizada, es necesario que sean específicas para que señalen certeramente las acciones que se deben implementar, mejorar o eliminar, el número de ellas depende directamente del resultado obtenido en el dictamen general; es decir, a menor control y/o mayor riesgo, corresponden más sugerencias.

Del Cuestionario Electrónico se generan sugerencias de las áreas de: *software, hardware*, redes, procedimientos administrativos, recursos humanos, recursos materiales e infraestructura, y del Programa Diagnóstico Automatizado se obtienen las recomendaciones realizadas a los equipos de cómputo y de comunicaciones; en relación a *software, hardware*, redes, bases de datos o *WEB*.

A continuación se presentan los posibles resultados:

5.4.2.1. Cuando el Dictamen es "*Aprobado":*

No se realiza ninguna Sugerencia, porque el negocio presenta un "Excelente" nivel de Control y Riesgo.

5.4.2.2. Cuando el Dictamen es "*Aprobado con Observaciones":*

Se realizan sugerencias porque el resultado es "Regular", debido a que se presentó en el dictamen general alguna de las siguientes combinaciones:

Cuestionario	Diagnóstico	Resultado
Regular	Regular	Regular
Deficiente	Excelente	Regular
Excelente	Deficiente	Regular

Si uno de los dos instrumentos de recolección de datos es "Excelente", no se realiza ninguna acción; pero sí el estado es "Regular o Deficiente" se debe identificar cual es y la sugerencia recomendada.

A continuación se presenta la mecánica o lógica empleada en la definición de variables en cada uno de los dos instrumentos de recolección:

a) Cuestionario Electrónico

Para definir las variables se consideran las tres áreas y siete subáreas que integran el cuestionario. Para facilitar su identificación se emplea el prefijo "sg" de "sugerencias" y las iniciales del área de estudio *(ver Fig. 88)*.

Figura 88. Variables de Sugerencias

Área de estudio	Variables
Tecnología – Software	Sg TS
Tecnología – Hardware	Sg TH
Tecnología - Redes	Sg TR
Gestión Administrativa - Recurso Humano	Sg GARH
Gestión Administrativa – Procedimientos	Sg GAP
Recursos Físicos – Infraestructura	Sg RFI
Recursos Físicos – Materiales	Sg RFM

Fuente: [Elaboración Propia]

Para considerar el 100% de las preguntas se agrupan en dos formatos distintos, el primero incluye las preguntas de tres incisos y el segundo las de múltiples respuestas. Formato 1. Se enfoca en las variables definidas en la figura 66."Variables de Respuestas con tres incisos", relacionadas a las preguntas del área de "*Tecnología con Software –TS*", para el diseño de la sugerencia correspondiente *(ver Fig. 89)*.

Figura 89. Sugerencias por incisos

No.	Pregunta	*Variable*	Sugerencias	*Variable*
1	Licencias de Software	TS1	Las licencias de Software deben ser privadas/gratuitas	Sg TS1
2	Sistema Operativo (servidores)	TS2	El sistema operativo para servidores debe ser Unix	Sg TS2
7	Administración de Base de Datos	TS7	El SGBD debe ser Oracle	Sg TS7
8	Análisis de virus	TS8	El análisis de virus debe ser Semanal	Sg TS8
9	Cambio de contraseñas	TS9	El cambio de contraseña debe ser Semanal	Sg TS9
10	Acceso Lógico	TS10	El control de Acceso lógico debe ser Método biométrico	Sg TS10
11	Control de equipo por usuario	TS11	El Control de equipo por usuario debe ser automatizado	Sg TS11
12	Periodo de respaldo de datos	TS12	El respaldo de la base de datos debe ser Diario	Sg TS12
18	Protocolos de seguridad	TS18	La aplicación de los protocolos de seguridad de internet debe ser diario	Sg TS18
21	Monitoreo actividades WEB	TS21	El Monitoreo de la Web debe ser automatizado	Sg TS21

Fuente: [Elaboración Propia]

Las sugerencias propuestas en las variables "SgTS(x)" son los incisos (A) de cada pregunta, partiendo de la premisa que contienen la opción deseable, que se aplicará literalmente si la respuesta seleccionada es (B) o (C).

Otra forma de abordar este análisis es recordar que (A) equivale a 3 puntos, (B) equivale a 2 puntos y (C) equivale a 1 punto. Por lo tanto, *si TS1 <> 3, entonces* aplica Sg TS1, de lo contrario *no aplican sugerencias.*

Formato 2. Se enfoca en las variables definidas en la figura 67. "Variables de Respuestas múltiples", relacionadas a las preguntas del área de "*Tecnología con Software –TS*", para el diseño de la sugerencia correspondiente, *(ver Fig. 90)*.

Figura 90. Sugerencias por opción múltiple

Núm.	Preguntas/ Respuestas	Variables	Sugerencias	Variables
3	Sistemas Operativos (PC)	TS3:=R1+R2+R3	Se recomienda instalar el sistema operativo:	Sg TS3
✓	Windows	R1=1		
	Linux	R2= 0	*Linux*	
✓	Solaris	R3=1		
4	Recursos de Software	TS4:=R1+R2+R3+R4+R5+R6+R7+R8+R9	Se recomienda incluir en la lista de recursos de software:	Sg TS4
✓	Procesador de Texto	R1=0.33		
✓	Hoja de Cálculo	R2=0.33		
✓	Base de Datos	R3=0.33		
✓	Editor de Presentaciones	R4=0.33		
	Editor de Videos	R5=0	*Editor de Videos*	
	Editor de folletos	R6=0	*Editor de folletos*	
	Editor de tutoriales	R7=0	*Editor de tutoriales*	
✓	Navegadores	R8=0.33		
✓	Buscadores	R9=0.33		
5	Limpieza del Sistema	TS5:= R1+R2+R3+R4+R5+R6	Se recomienda instalar Software que detecten y eliminen:	Sg TS5
✓	Adwares	R1=0.5		
	Spyware	R2=0	*Spyware*	
✓	Malware	R3=0.5		
✓	Virus	R4=0.5		
✓	Troyanos	R5=0.5		
✓	Gusanos	R6=0.5		
6	Administración del Sistema	TS6:= R1+R2+R3+R4	No hay sugerencia	
✓	Memoria Virtual y Cache	R1=0.75		

✓	Privilegios y funciones de Usuarios	R2=0.75		Sg TS6
✓	Actividades en red local o remota	R3=0.75		
✓	Otros	R4=0.75		
13	Control de Transacciones en Bases de Datos:	TS13:= R1+R2+R3+R4+ R5	Con la finalidad de mejorar el control de transacciones se recomienda :	
✓	Software de Auditoria de BD	R1=0.6		Sg TS13
✓	Restricciones de integridad	R2=0.6		
✓	Control de concurrencia	R3=0.6		
	Protocolos en Recuperación de datos	R4=0	*Protocolos en Recuperación de datos.*	
	Permisos en cuentas de usuarios	R5=0	*Permisos en cuentas de usuarios*	
14	Protocolos de Recuperación de Datos	TS14:= R1+R2+R3	Se recomienda incluir en la Recuperación Datos, los siguientes protocolos:	
✓	Contratación de servicios externos	R1=1		Sg TS14
✓	A nivel Software (Recuva, Easy Drive Data Recovery)	R2=1		
	A nivel Código (paginación de Sombra, RAID)	R3=0	*A nivel Código (por ejemplo: paginación de Sombra, RAID)*	
15	Protección de Datos del nivel Alto	TS15:=R1+ R2+R3+R4+ R5+R6	Se recomienda proteger los siguientes datos pertenecientes al nivel alto de seguridad:	Sg TS15
✓	Ideología	R1=0.5		
✓	Religión	R2=0.5		
✓	Creencias	R3=0.5		
✓	Origen racial	R4=0.5		
	Salud	R5=0	Salud	
	Vida Sexual	R6=0	Vida Sexual	

Fuente [Elaboración propia].

Las sugerencias propuestas en las variables "SgTS(x)" se obtienen de la acumulación de opciones no seleccionadas; partiendo de la premisa que la respuesta deseable es aquella que incluye a todas.

Por ejemplo, SgTS15 quedaría de la siguiente manera: *"Se recomienda proteger los siguientes datos pertenecientes al nivel alto de seguridad: Salud y Vida Sexual".*

Una respuesta presenta una sugerencia cuando no alcanza la puntuación máxima de tres puntos; y una forma de detectar si le corresponde o no, es acumular en una variable la puntuación total de cada opción.

Por ejemplo, TS15:= R1+ R2+ R3+ R4+ R5+ R6, en donde cada R se le asigna la fracción correspondiente a 0.5 si fue seleccionada; y en caso contrario sería 0. Es importante señalar que cada pregunta tiene números de opciones diferentes por lo tanto el valor de cada R cambia en cada una. Pero, en base a este ejemplo se explica la asignación de 0.5 a cada R.

El número de opciones seleccionadas * tres (que es la puntuación máxima permitida) entre el total de opciones que incluya la respuesta. Ahora bien, *Si TS15 <> 3, entonces* aplica Sg TS15 incluyendo las R que tienen 0, en caso contrario *no aplican sugerencias.*

b) Programa Diagnóstico Automatizado

Para definir las variables se consideran los tres atributos y los intervalos que fueron definidos en la figura 85. "Dictamen por Intervalos de Atributos".

Los intervalos que se presentan son tres, el primero inicia en 115 y termina en 170 y corresponde a la escala de "Excelente", el segundo inicia en 58 y termina en 114 y corresponde a la escala de "Regular" y el último inicia en 0 y termina en 57 y corresponde a la escala más baja de "Deficiente".

El rango de cada uno fue determinado por la división del total de programas instalados entre tres (que representa el número de estados [E][R][D]).

De la misma manera se pueden agregar más atributos de estudio y enriquecer la auditoría. Las variables también incluyen el prefijo "sg" de sugerencias y las iniciales de cada atributo *(ver Fig. 91).*

Figura 91. Sugerencias por atributos

Atributos	Puntos:	Condición :	Sugerencias	Variable
Código del Paquete	*PC= 66*	Si 115>PC>57	Se recomienda que el número de *Código de Paquete* de los programas instalados sea mayor que 2/3, del total.	SgPC
Id del Producto	*PI= 3*	Si PI<58	Se recomienda que el número de *Identificador del Producto* de los programas instalados sea mayor que 1/3 del total	SgPI
Id del Software	*SI=168*	Si SI>114	No aplica	SgSI

Fuente: [Elaboración propia]

La condición se basa en tres posibles estados y se aplican a los tres atributos PC, PI y SI, de la siguiente manera:

- Si (atributo-puntos) es mayor que 114, entonces "no se aplican sugerencias".
- Si (atributo-puntos) es mayor que 57 y menor que 115, entonces "se recomienda que el número de atributo de los programas instalados sea mayor que 2/3, del total.
- Si (atributo-puntos) es menor que 58, entonces "se recomienda que el número de atributo de los programas instalados sea mayor que 1/3, del total.

Retomando el dictamen resultante del ejercicio real, el código del paquete obtuvo el estado de "Regular", el id del producto "Deficiente" y el id de *software* "Excelente". Por lo tanto, solo se realizan sugerencias para Código del paquete y para Id del producto.

Las fracciones de (2/3) y (1/3) representan la parte proporcional de cada intervalo; es decir, si los puntos oscilan entre 0 y 57 solo alcanzó una tercera parte del total deseado, si los puntos se encuentran entre 58 y 114 cubre dos terceras partes y si los puntos se ubican en el rango superior de 115 a 170 no se aplica sugerencias porque tiene cumple con 3/3.

5.4.2.3. Cuando el Dictamen es "*No Aprobado*"

Se realizan sugerencias en forma general, debido a que el resultado del dictamen se encuentra en estado "Deficiente". El criterio de evaluación aplicable indica que si se obtiene en las dos áreas [D] y [D] o si se obtiene en una [D] y en otra [R] el resultado será No Aprobado.

Para corroborar dicha información se pueden ver los criterios establecidos en la sección 5.4.1.3. "Dictamen General de Auditoría en Informática" y las combinaciones posibles son:

CUESTIONARIO	PROGRAMA	RESULTADO
Regular	Deficiente	Deficiente
Deficiente	Regular	Deficiente
Deficiente	Deficiente	Deficiente

a) Cuestionario Electrónico

Para definir las sugerencias primero se consideran las variables que acumulan los puntos alcanzados por cada área y subárea correspondiente, asimismo, se señalan los intervalos con el rango inferior para aplicar la condición lógica que le corresponde a la escala "Deficiente" *(ver Fig. 92)*.

Figura 92. Intervalos con Escala Deficiente

área:	Variables	Intervalos	Condición	Escala
Tecnología	TTEC	77-114 39-76 **0-38**	***Si TTEC < 39***	Excelente Regular **Deficiente**
Software	Stotal	43-63 22-42 **0-21**	***Si Stotal < 22***	Excelente Regular **Deficiente**
Hardware	Htotal	21-30 11-20 **0-10**	***Si Htotal < 11***	Excelente Regular **Deficiente**
Redes	Rtotal	16-23 8-15 **0-7**	***Si Rtotal < 8***	Excelente Regular **Deficiente**
Gestión Administrativa	TGA	71-105 36-70 **0-35**	***Si TGA < 36***	Excelente Regular **Deficiente**
Recurso Humano	RHtotal	23-33 12-22 **0-11**	***Si RHtotal < 12***	Excelente Regular **Deficiente**
Procedimientos	PROtotal	49-72 25-48 **0-24**	***Si PROtotal< 25***	Excelente Regular **Deficiente**
Recursos Físicos:	TRF	55-81 30-54 **0-29**	***Si TRFA < 30***	Excelente Regular **Deficiente**
Infraestructura	INFtotal	29-42 15-28 **0-14**	***Si INFtotal < 15***	Excelente Regular **Deficiente**
Material	MATtotal	27-39 14-26 **0-13**	***Si MATtotal < 14***	Excelente Regular **Deficiente**

Fuente: [Elaboración propia]

Cuando ya se han identificado los datos, se compara la puntuación obtenida de la aplicación del cuestionario electrónico en un ambiente real (ver figura 81. Dictamen por intervalos del Cuestionario [Subáreas] con la condición lógica), y se observa que los puntos obtenidos no entran en el rango inferior, por lo tanto la condición no se cumple y no se pueden aplicar sugerencias.

Por ejemplo:

- En el área de Tecnología se obtuvieron (44.5 puntos) en Software, (20.05 puntos) en Hardware y (17.0 puntos) en Redes, ninguna se encuentra en el intervalo Deficiente, por lo tanto no aplican sugerencias.
- En el área de Gestión Administrativa se obtuvieron (20.63 puntos) en Recurso Humano y (52.32 puntos) en Procedimientos, ninguna se encuentra en el intervalo Deficiente, por lo tanto no aplican sugerencias.
- En el área de Recursos Físicos se obtuvieron (24.95 puntos) en Infraestructura y (23.3 puntos) en Material, ninguna se encuentra en el intervalo Deficiente, por lo tanto no aplican sugerencias.

Si se modifica la puntuación del área de Tecnología y las subáreas correspondientes *(ver Fig. 93)*, para observar la actuación de la condición, cuando ésta se cumple; quedaría de la siguiente manera:

Figura 93. Sugerencias Generales

	área:	**Puntos**	**condición :**	**Sugerencia**
1	**Tecnología**	38	***Si TTEC < 39***	*Se recomienda mejorar los procedimientos actuales en el área de Tecnología e implementar nuevos mecanismos de control en:*
	Software	20	***Si Stotal < 22***	Software
	Hardware	11	***Si Htotal < 11***	**No aplica**
	Redes	7	***Si Rtotal < 8***	Redes

Fuente: [Elaboración propia]

Entonces la sugerencia propuesta almacenada en la variable SgTTEC, quedaría: "Se recomienda mejorar los procedimientos actuales en el área de Tecnología e implementar nuevos mecanismos de control en las subáreas de *Software y Redes*".

Es decir, puede crearse una plantilla y modificar solo los campos afectados, de la siguiente manera: "*Se recomienda mejorar los procedimientos actuales en el área de [nombre-área] e implementar nuevos mecanismos de control en las subáreas de: [nombre-sub-área1]+…+[nombre-sub-área(n)]*".

Se aplicaría la misma sugerencia, aun cuando el estado del Cuestionario Electrónico sea "Regular"; basado que el Dictamen General ya que el resultado final fue "Deficiente".

b) Programa Diagnóstico Automatizado

Las variables de las sugerencias son "SgPC", "SgPi" y "SgSi" y se aplican cuando el programa presenta un dictamen "Deficiente", se debe a la presencia de una [D], en cualquiera de los siguientes casos:

- La presencia de una [D] en los tres atributos;
- una [D] en dos atributos y una [E] o [R] en otro.
- una [D] en cualquier atributo y en los otros dos [R].

En este caso, "*Se recomienda una mejora total en los atributos evaluados: Código del Paquete, Identificador del Producto e Identificador del Software*".

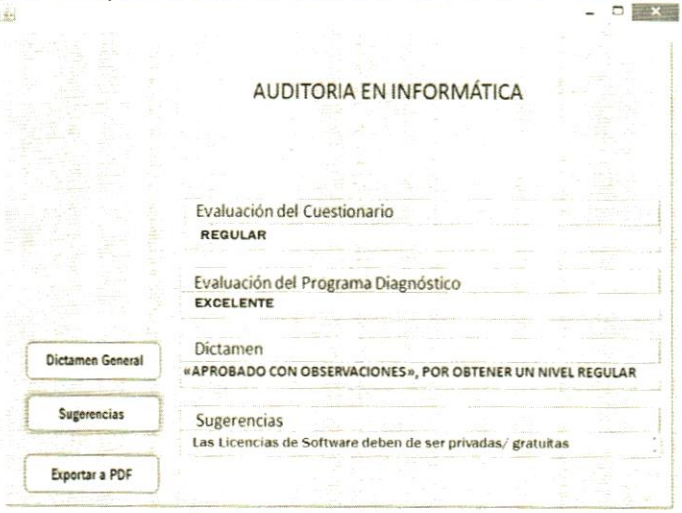
Se aplicaría la misma sugerencia, aun cuando el estado del Programa Diagnóstico Automatizado sea "Regular"; basado que el Dictamen General ya que tiene como resultado final "Deficiente".

De esta manera se concluye la Metodología para el desarrollo de un Sistema Gerencial de Auditoría en Informática que genera un Dictamen y Sugerencias en forma Automatizada.

Apéndice 1. Dictamen *Aprobado con Observaciones [Cuestionario Electrónico]*

Se presenta la documentación que se entrega a la organización auditada, que consiste en archivos en formato PDF que contienen el Dictamen de la Auditoría en Informática y las Sugerencias correspondientes al Cuestionario Electrónico. Siempre y cuando el resultado de la evaluación sea "Regular" y la del Programa Diagnóstico Automatizado sea "Excelente", como se aprecia en la figura siguiente *(ver Fig. 94)*.

Figura 94. Aprobado con observaciones en Cuestionario Electrónico



Fuente [Pantalla del Programa]

El Dictamen debe contener los siguientes datos *(ver Fig. 95)*.

- Fecha y Lugar
- Nombre de la Empresa
- Responsable de la Empresa
- Puesto que ocupa en la Empresa
- Responsable del Área de Cómputo o Informática.
- Resultado del Dictamen
- Auditor Responsable.

Las sugerencias deben ser presentadas en forma clara y específica *(ver Fig. 96)*.

Figura 95. Dictamen General de Auditoría en Informática [PDF]

Fecha.
lugar.

[EMPRESA]
[Responsable de la Institución]
Dirección.

AT'N. [Responsables del Área]
Centro de Cómputo.

Por medio de la presente, se informa el Dictamen de Auditoria en Informática, realizada en la empresa que Usted dignamente representa:

« APROBADO CON OBSERVACIONES»

Con un Nivel REGULAR, en las evaluaciones realizadas a los controles internos.

Con la finalidad de cumplir con el compromiso del Grupo Auditor, se anexan las Recomendaciones orientadas a disminuir los riesgos existentes y fortalecer la administración de Tecnología de Información y Comunicaciones en el área de informática.

[Auditor Responsable]

1/2

Fuente [Pantalla PDF del programa]

Figura 96. Sugerencias del Cuestionario Electrónico [PDF]

Fecha.
lugar.

[EMPRESA]
[Responsable de la Institución]
Dirección.

AT'N. [Responsables del Área]
Centro de Cómputo.

RECOMENDACIONES:

EN PROCEDIMIENTOS:

- Se recomienda que las licencias de Software deben de ser privadas/ gratuitas.
- Se recomienda que el análisis de virus debe ser semanal.
- Se recomienda que el respaldo de la base de datos debe ser Diario.
- Se recomienda que el Monitoreo de la Web debe ser automatizado
- Se recomienda instalar el sistema operativo: Linux
- Se recomienda incluir en la lista de recursos de software: Editor de Videos, Editor de folletos, Editor de tutoriales.
- Se recomienda instalar Software que detecten y eliminen: Spyware
- Se recomienda con la finalidad de mejorar el control de transacciones: Protocolos en Recuperación de datos.
- Se recomienda incluir en la recuperación de datos los siguientes protocolos: a nivel código (p.e. paginación en sombra, RAID).
- Se recomienda proteger los siguientes datos por considerar en el nivel alto de seguridad: salud y vida sexual.

EN DIAGNÓSTICO DEL EQUIPO:

- No aplican recomendaciones.

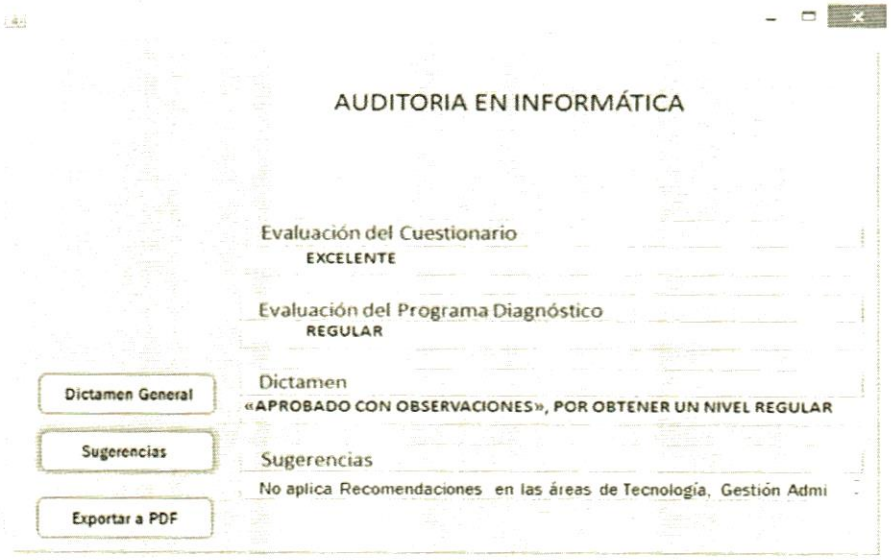
2/2

Fuente [Pantalla PDF del programa]

Apéndice 2. Dictamen *Aprobado con Observaciones [Programa Diagnóstico Automatizado]*

Presenta la documentación que se entrega a la organización auditada, que consiste en archivos en formato PDF que contienen el Dictamen de la Auditoría en Informática y las Sugerencias correspondientes al Programa Diagnóstico Automatizado. Siempre y cuando el resultado de la evaluación sea "Regular" y la del Cuestionario Electrónico sea "Excelente", como se aprecia en la figura siguiente *(ver Fig. 97)*.

Figura 97. Aprobado con Observaciones en Programa Diagnóstico Automatizado



Fuente [Pantalla del Programa]

El Dictamen es igual al presentado en la figura 95, lo que variará serán las sugerencias por que presenta información diferente, pero se mantiene el mismo criterio sobre la forma de presentación, ésta debe ser clara y específica *(ver Fig. 98)*.

Figura 98. Sugerencias del Programa Diagnóstico

Fecha.
lugar.

[EMPRESA]
[Responsable de la Institución]
Dirección.

AT'N. [Responsables del Área]
Centro de Cómputo.

RECOMENDACIONES:

EN PROCEDIMIENTOS:

- No aplica Recomendaciones en las áreas de Tecnología, Gestión Administrativa y Recursos Físicos relacionados con el manejo y control de los sistemas computacionales.

EN EL DIAGNÓSTICO DEL EQUIPO:

- Se recomienda que el número DE CÓDIGO DEL PAQUETE de los programas instalados, sea mayor que 2/3 del total.

- Se recomienda que el número DE IDENTIFCADOR DEL PRODUCTO de los programas instalados, sea mayor que 1/3 del total.

[Auditor Responsable]

_____

2/2

Fuente [Pantalla PDF del programa]

Bibliografía

Alberto, R. A. (07 de febrero de 2011). Sarbanes Oxley e IT, una relación que rompe corazones y nervios. Página electrónica recuperado el 29 de marzo de 2013, disponible en http://www.bsecure.com.mx/opinion/sarbanes-oxley-e-it-una-relacion-que-rompe-corazones-y-nervios

ApexSQL (2014). Discovery and recovery tool. Explore the SQL transacion log and undo transactions Audit Schema and data changes Página electrónica recuperado el 05 de junio del 2014, disponible en http://www.apexsql.com/sql_tools_log.aspx

Buscador de Patentes en México (INFOPAT). Página electrónica recuperado el 02 de octubre del 2013, disponible en http://www.infopat.com.mx/#

Banco Nacional de Marcas (MARCANET). Página electrónica recuperado el 09 de octubre del 2013, disponible en http://marcanet.impi.gob.mx/marcanet/controler/ExpedienteDespliega/_expediente/

Call Center, México. Página electrónica Recuperado el 12 de 03 de 2014, disponible en http://www.callcentermexico.com.mx/

Código de Comercio (10 de enero del 2014). Cámara de Diputados del H. Congreso de la Unión, Secretaría de Servicios Parlamentarios. Página electrónica recuperado el 01 de marzo del 2014, Disponible en http://www.diputados.gob.mx/LeyesBiblio/pdf/3.pdf

Código Civil Federal (26 de diciembre del 2011). Cámara de Diputados del H. Congreso de la Unión, Secretaría de Servicios Parlamentarios. Página electrónica recuperado el 22 de agosto del 2013, disponible en http:// www.diputados.gob.mx/LeyesBiblio/pdf/2.pdf

Código Fiscal de la Federación (12 de diciembre del 2011). Cámara de Diputados del H. Congreso de la Unión, Secretaría de Servicios Parlamentarios. Página electrónica recuperado el 20 de octubre del 2013, disponible en http://www.diputados.gob.mx/LeyesBiblio/pdf/8.pdf

Código Penal Federal (26 de diciembre del 2013). Cámara de Diputados del H. Congreso de la Unión, Secretaría de Servicios Parlamentarios. Página electrónica recuperado el 22 de febrero del 2014, disponible en http://www.diputados.gob.mx/LeyesBiblio/ref/cpf.htm

Constitución Política de los Estados Unidos Mexicanos (30 de 09 de 2013). Recuperado el 05 de 10 de 2013, de Cámara de Diputados del H. Congreso de la Unión, Secretaría de Servicios Parlamentarios. Página electrónica recuperado el 27 de febrero del 2014, disponible en http://www.diputados.gob.mx/LeyesBiblio/pdf/1.pdf

Contrato de Términos y Condiciones de TELMEX (23 de diciembre de 1947). Página electrónica recuperado el 04 de octubre del 2013, disponible en https://pvalores.telmex.com/.../Terminosycondiciones_Infinitum11_12.pdf

Contrato de Términos y Condiciones de Mercado Libre (19 de octubre del 2012). Página electrónica recuperado el 25 de febrero del 2014, disponible en http://ayuda.mercadolibre.com.mx/seguro_terminos

Creative Commons (2013). Página Electrónica recuperado el 01 de septiembre del 2013, disponible en http://creativecommons.org/choose/

Danilo, L. C. (30 de julio de 2002). Frente a los Fraudes Contables. Página electrónica recuperado el 29 de marzo de 2013, disponible en http://www.interamericanusa.com/articulos/Leyes/Ley-Sar-Oxley.htm

Díaz, F. J., Harari, I., & Amadeo, A. P. (2007). Hacia una Interfaz Accesible: Experiencia sobre un portal educativo. IX Workshop de Investigadores en Ciencias de la Computación, (pág. 4). Buenos Aires.

Echenique, J.A. (2000). Auditoría en Informática, Editorial Mc Graw Hill, México. D.F. Pp.16

Extintores Nacionales. Asesoramiento en Seguridad Industrial y Equipos Automáticos contra Incendio, Página electrónica recuperado el 12 de diciembre del 2013, disponible en http://www.extintoresnacionales.com/productos-extintores-de-fuego-portatiles-moviles-automaticos-equipos-de-bombero-monterrey

FreshDiagnose. Softonic. Página electrónica recuperado el 04 de abril del 2014, de http://fresh-diagnose.softonic.com/

Fundación Copyleft (2013). Página electrónica recuperado el 29 de agosto del 2013 disponible en http://fundacioncopyleft.org/es

Graniel Ortega, P. (12 de junio 2014). iFone vs iPhone ¿Absurdo o brillante?. Página electrónica recuperada el 25 de agosto del 2014, disponible en http://yeux.com.mx/ColumnaUniversitaria/ifone-vs-iphone-absurdo-o-brillante/

Instituto Mexicano de la Propiedad Industrial (IMPI). Página electrónica recuperado el 23 de agosto del 2013, disponible en http://www.impi.gob.mx/

Instituto Nacional del Derecho de Autor (INDAUTOR). Página electrónica recuperado el 28 de agosto del 2013, disponible en http://www.indautor.gob.mx/ formatos/registro/ obra_computo.html

Internet Corporation for Assigned Names and Numbers (ICANN). Página electrónica recuperado el 20 de agosto del 2013, disponible en https://www.icann.org/resources/pages/listing

Jiménez, X. (11 de enero del 2013). El Periódico.com. Vecinos comparten la red, liberad a wifi. Página electrónica recuperado el 18 de julio del 2013, disponible en http://blogs.elperiodico.com/masdigital/afondo/ vecinos-2-0-comparten-la-red-liberad-a-wifi

Ley de la Propiedad Industrial en México (09 de abril del 2012). Cámara de Diputados del H. Congreso de la Unión, Secretaría de Servicios Parlamentarios. Página electrónica recuperado el 27 de agosto del 2013, disponible en http://www.diputados.gob.mx/LeyesBiblio/pdf/ 50.pdf

Ley Federal de Derechos de Autor en México (10 de junio del 2013). Cámara de Diputados del H. Congreso de la Unión, Secretaría de Servicios Parlamentarios. Página electrónica recuperado el 25 de agosto del 2013, disponible en http://www.diputados.gob.mx/ LeyesBiblio/pdf/ 122.pdf

Ley Federal de Protección al Consumidor (16 de enero del 2013). Cámara de Diputados del H. Congreso de la Unión, Secretaría de Servicios Parlamentarios. Página electrónica recuperado el 28 de agosto del 2013, disponible en http://www.profeco.gob.mx/juridico/pdf/ LFPC_actuali_16ene2013.pdf

Ley Federal de Protección de Datos (05 de julio del 2010). Cámara de Diputados del H. Congreso de la Unión, Secretaría de Servicios Parlamentarios. Página electrónica recuperado el 28 de agosto del 2013, disponible en http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

Ley Federal de Telecomunicaciones (16 de enero del 2013). Cámara de Diputados del H. Congreso de la Unión, Secretaría de Servicios Parlamentarios. Página electrónica recuperado el 29 de agosto del 2013, disponible en http://www.diputados.gob.mx/LeyesBiblio/pdf/118.pdf

López Varas, M. (2010). Regulación Jurídica de la Contratación Electrónica en el Código Civil Federal, Toluca, México. 1a.Ed. ISBN 978 607 95328-5-7

Maulini R, M. Seguridad banca por Internet, e-Securing. Página electrónica recuperado el 11 de julio del 2014, disponible en http://www.e-securing.com/novedad.aspx?id=66

Michel, E. (2014 de 06 de 06). El Universal. Gana Mexicana Ifone batalla legal a Iphone. Recuperado el 06 de agosto del 2014, disponible en http://www.eluniversal.com.mx/nacion-mexico/2014/gana-mexicana-ifone-batalla-legal-a-iphone-1015398.html

Microsoft, Windows. (2013). Configurar una clave de seguridad para una red inalámbrica. Página electrónica recuperado el 23 de septiembre de 2013, disponible en http:/windows.microsoft.com/esxl/windows7/set-up-a-security-key-for-a-wireless-network

Muñoz Razo, C. (2002). Auditoría en Sistemas Computacionales, Pearson Educación, México. Pp. 23

Networks Information Center, México (NIC). Página electrónica recuperado el 20 de septiembre del 2013, disponible en http://www.nic.mx/es/NicMx.Divisiones/RegistryMx

Nessus. (2014). Vulnerability Scanner. Tenable Networks Security. Página electrónica recuperado el 08 de junio de 2014, disponible en http://www.tenable.com/products/nessus/nessus

Nmap 6.25. (03 de diciembre de 2012). Softonic. Página electrónica recuperado el 06 de 06 de 2014, de José MAría López: http://nmap.softonic.com/

Onofre, J. S. (10 de febrero del 2013). El Economista, Ifone vs Apple. Página electrónica recuperado el 09 de setiembre del 2013, disponible en http://eleconomista.com.mx/tecnociencia/2013/02/10/ ifone-vs-apple-historia-juridica

OpenAudit. Softpedia. Página electrónica recuperado el 02 de marzo de 2014, disponible en http://webscripts.softpedia.com/script/ Networking-Tools/ Open-udIT-36429.html

Organismo Mundial de la Propiedad Intelectual (OMPI). Página electrónica recuperado el 23 de agosto del 2013, disponible en http://www.impi.gob.mx/

Quecalor.com. Página electrónica recuperado el 10 de octubre del 2013, disponible en http://www.quecalor. com/aire-acondicionado-calculo.php

Ramírez López,D. & Espinoza Madrigal, C.(2011). El Cifrado Web (SSL/TLS). Seguridad, Cultura de prevención para TI, UNAM, UNAM_CERT, Página electrónica recuperado el 23 de septiembre del 2013, disponible en, http://revista.seguridad.unam.mx/numero-10/el-cifrado-web-ssltls

Reforma en Materia de Telecomunicaciones (02 de diciembre del 2012). Pacto por México. Página electrónica recuperado el 05 de octubre del 2013, disponible en http://pactopormexico.org/reforma-telecomunicaciones/

Remixado, Q. (02 de enero de 2012). Mafalda te explica la Ley SOPA. Página electrónica recuperado el 29 de marzo del 2014, disponible en http://derechoaleer.org/blog/2011/11/infografia-otra-vez-sopa.html

Rodriguez Barrios, J. 2005. Modelo de gestión auditable para instalación, operación y mantenimiento de switches y routers. Telematique: Revista Electrónica de Estudios Telemáticos. ISSN 8156-4194, Vol 4, N°1, Pp. 29-49.

SecureAuditor. Softpedia. Página electrónica recuperado el 04 de junio de 2014, disponible en http://www.softpedia.es/programa-Secure-Auditor-98177.html

SecureSqlAuditor. Secure Bytes, synonymous with digital security. Página electrónica recuperado el 04 de junio del 2014, disponible en http://download.cnet.com / Secure-SQL-Auditor / 3000 – 2653 _ 4 - 7568 3319.html

Softkey. Softonic. Página electrónica recuperado el 05 de abril del 2014, disponible en http://softkey-revealer.softonic.com/

Tamayo Alzate, A. (2001). Auditoría de Sistemas, una visión práctica. Universidad de Colombia, Manzanales, Colombia.

TAW. Sedic. Página electrónica recuperado el 03 de junio del 2014, disponible en http://www.sedic.es/autoformacion/accesibilidad/9-tecnicas-herramientas.html

Teléfonos de México S.A.B. de C.V. (TELMEX). Página electrónica recuperado el 30 de agosto del 2013, disponible en http://192.168.1.254

Total Network Inventory. Softinventilab. Página electrónica recuperado el 10 de marzo de 2014, disponible en http://www.softinventive.es/total-network-inventory/

Watobo. (25 de 02 de 2011). Cryptex. Seguridad de la Información. Página electrónica recuperado el 07 de junio del 2014, disponible en http://seguridad-informacion.blogspot.mx/2011/02/watobo-herramienta-de-auditorias-de.html

Watobo. (11 de julio de 2012). Sourceforge.net. Página electrónica recuperado el 07 de junio de 2014, disponible en http://sourceforge.net/apps/mediawiki/watobo/index.php?title=Videos#Video_Tutorials

WhatWeb. (05 de abril del 2011). Morningstar security. Página electrónica recuperado el 03 de junio de 2014, disponible en http://www.morningstarsecurity.com/research/whatweb

WireShark. Softonic. Página electrónica recuperado el 05 de mayo del 2014, disponible en http://wireshark.softonic.com/

WinAudit. Softpedia. Página electrónica recuperado el 04 de abril del 2014, disponible en: http://www.softpedia.es/programa-WinAudit-11148.html

W3C (15 de diciembre del 2009). WCAG 2.0. Web Content Accessibility Guidelines. Página electrónica recuperado el 03 de junio del 2014, disponible en http://www.sidar.org/traducciones/wcag20/es/

XRumer (25 de noviembre del 2013). Submitter 4 elites. Página electrónica recuperado el 04 de junio del 2014, disponible en http://xrumersubmitter4elites.blogspot.mx/

AUDITORIA EN INFORMÁTICA,
ASISTIDA POR TECNOLOGIA
CON DICTÁMEN Y SUGERENCIAS

Se terminó de imprimir en el mes de noviembre de 2014,
con un tiraje de 500 ejemplares, la impresión estuvo a cargo
del Taller de Publicaciones del SPAUNACH, ubicado en 16a.
Pte. Sur No. 326, Col. Xamaipak, C.P. 29060,
Tuxtla Gutiérrez, Chiapas.

La Auditoría en Informática, entendida como el proceso de supervisión y evaluación de los controles de operación y administración de los equipos computacionales y las tecnologías de información y comunicación, también se extiende a la relación existente entre la estructura, los recursos materiales y los humanos disponibles en una organización; asimismo, involucra el grado de seguridad y los niveles de cumplimiento del marco legal regulatorio, indispensables para la emisión del dictamen y las recomendaciones derivadas de los procesos de revisión, orientados a la disminución de riesgos y aseguramiento de acciones para la mejora continua.

Los auditores coinciden, que independientemente del alcance establecido, la auditoría es un proceso laborioso, resultado del volumen de información que debe evaluarse, en donde la experiencia y habilidad del auditor resultan factores importantes al momento de seleccionar las técnicas y herramientas de apoyo para la recolección y análisis de datos, así como en la elección del método para la interpretación de resultados; logrando con ello optimizar los recursos utilizados al desarrollar esta importante actividad.

En esta obra, la autora ofrece a estudiantes universitarios y en general a profesionales interesados en esta área, una alternativa para realizar la Auditoría en Informática, asistida por tecnología, basándose en el diseño de metodología específica, apoyada en el desarrollo de un Sistema Experto de Evaluación, que emplea como datos de entrada los reportes emitidos por los programas de diagnóstico para computadoras y redes de comunicación existentes y los resultados generados por cuestionario automatizado para obtener imparcialmente un dictamen y a partir de él, generar las sugerencias que resultan necesarios para optimizar el empleo de los recursos informáticos.

Con esta obra se aporta un eslabón en la cadena cognitiva que impulsa la generación y aplicación de conocimientos en la disciplina informática y en el ámbito del Desarrollo Organizacional.

ISBN: 978-607-8304-21-9

Auditoría en Informática asistida por tecnología, con dictamen y sugerencias

Carmen Carolina Ortega Hernández

Generación y Gestión para la Innovación
Edición 2014

Libro financiado con recursos del PIFI