UNIVERSIDAD AUTÓNOMA DEL ESTADO DE MÉXICO.

Centro Universitario UAEM Texcoco.

“LA SEGURIDAD INFORMÁTICA EN LA LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LOS PARTICULARES”

TESINA

QUE PARA OBTENER EL GRADO DE

LICENCIADO EN INFORMÁTICA ADMINISTRATIVA

PRESENTA:

BARREIRO NEYRA ALMA IRAIS

DIRECTOR

M. en C. CARLOS OCELOTL RIVERA VILLA

REVISORES

M. en C. ANA LUISA MARTINEZ AVIDA

ING. FERNANDO ROBLES GIL

TEXCOCO ESTADO DE MÉXICO 2013

AGRADECIMIENTOS

A MI HIJA XIMENA ITZAYANA

POR SER MI PRINCIPAL MOTIVACIÓN,

HABER LLENADO MI VIDA DE LUZ Y FELICIDAD,

POR SER HERMOSA, AMOROSA Y MUY INTELIGENTE.

ESTO ES POR TI BEBE Y ES UN TRIUNFO DE AMBAS,

GRACIAS POR TU COMPRENSIÓN Y TU TIEMPO.

TE AMO NENA.

A MI MADRE

POR SER UN EJEMPLO A SEGUIR,

POR BRINDARME SU APOYO INCONDICIONAL,

SU COMPRENSIÓN, AYUDA Y TOLERANCIA.

POR ESTAR SIEMPRE A MI LADO

Y DARME LA FORTALEZA PARA SEGUIR

ADELANTE ANTE CUALQUIER CIRCUNSTANCIA.

GRACIAS MAMI

A MI ESPOSO Y FAMILIA

POR BRINDARME SU TIEMPO,

Y SUS PALABRAS DE ALIENTO,

GRACIAS POR SUS BUENOS CONSEJOS Y SU AYUDA.

GRACIAS A TODOS.

A MI DIRECTOR DE TESINA

M. en C. CARLOS OCELOTL RIVERA VILLA

POR SUS SABIOS CONSEJOS,

Y HABER COMPARTIDO CONMIGO SU

TIEMPO Y SUS CONOCIMIENTOS,

POR HABER RESPONDIDO TODAS LAS DUDAS

QUE FUERON SURGIENDO AL DESARROLLAR EL TRABAJO,

POR SUS PALABRAS DE ALIENTO Y

LA CONFIANZA QUE ME BRINDO

GRACIAS POR AYUDARME

A CUMPLIR ESTA META.

A MIS REVISORES

M. en C. ANA LUISA MARTÍNEZ AVIDA

ING. FERNANDO ROBLES GIL

POR HABERME APOYADO CON SU TIEMPO

Y SUS BUENAS OBSERVACIONES,

POR HABER DISIPADO MIS DUDAS Y HACER

QUE ESTE TRABAJO SEA UNA REALIDAD,

GRACIAS POR SU AYUDA

Índice General

Introducción

Actualmente el uso de la información se ha vuelto imprescindible, es un recurso fundamental en el funcionamiento de las organizaciones como pueden ser empresas e instituciones educativas, la gran parte de las personas trabajan con palabras, números e ideas que constituyen la información que se representa y almacena como una serie de bits.

Toda información con la que se trabaja diariamente debe de estar vigilada y brindar un nivel de seguridad para su tratamiento y control, tomando en cuenta que no existe una seguridad absoluta, es necesario minimizar el impacto o el riesgo de robo, así como el uso inadecuado de dicha información.

Tanto las instituciones gubernamentales como las empresas privadas acumulan información acerca de nuestras identidades, y gracias a la existencia de redes se facilitan las transmisiones, comparticiones y fusión de dicha información. Tomando en consideración lo anterior, existe la preocupación de una amenaza a la privacidad, ya que se confía ciegamente en el uso correcto de datos personales y la seguridad que se le dé a dicha información.

En consecuencia, se decretó la Ley federal de protección de datos personales en posesión de los particulares, publicada en el Diario Oficial de la Federación (DOF) el 5 de julio de 2010, cuyo propósito principal es proteger el derecho a la privacidad individual de los datos recopilados por las empresas privadas.

Para el correcto cumplimiento de esta Ley y contribuir a dar tratamiento, control y privacidad a la información, es necesaria la seguridad informática y la seguridad de la información por ser el conjunto de medidas tomadas para proteger datos o información contra robos, ataques, crímenes, espionajes o sabotajes.

Muchas veces las empresas privadas no le dan la debida importancia a la protección de los datos personales de clientes, empleados o proveedores y por lo tanto, no contratan a personal especializado para vigilar y controlar el trato de la información, y como consecuencia se hace mal uso de estos datos de suma importancia.

El presente trabajo tiene como objetivo analizar y conocer la ley federal de protección de datos personales en posesión de los particulares, para garantizar la implementación y el cumplimiento de la misma, así como investigar la función de la seguridad de la información de los particulares mediante la consideración de la importancia que se debe dar a la información privada de terceros, no solo para el cumplimiento satisfactorio de la Ley, sino porque la inseguridad aumenta día con día y si se da un uso inadecuado a la información que voluntariamente se confía a un empresa se pone en riesgo la integridad de las personas.

El trabajo consta de cuatro capítulos, además de las conclusiones y bibliografía. En el primer capítulo se exponen los antecedentes de la seguridad informática, se revisan los conceptos; de informática, seguridad, así como los tipos de vulnerabilidad y de riesgos, los objetivos de la seguridad informática y las razones para implementarla en una empresa.

En el segundo capítulo se da una amplia explicación de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, sus disposiciones generales, de igual forma se definen los datos personales, los datos sensibles, el aviso de privacidad; los derechos de Acceso, Rectificación, Cancelación, y Oposición (ARCO), se define el aviso de privacidad, y las sanciones a las que se harán acreedoras las empresas que no cumplan con la Ley, según el Instituto Federal de Acceso a la Información (IFAI) encargado de vigilar el cumplimiento de la Ley.

En el tercer capítulo se hace una descripción de los modelos de arquitecturas diseñados e implementados para vigilar la seguridad de la información en una empresa, comienza con la definición de arquitectura de seguridad de la información y menciono algunos tipos de arquitecturas como son: Arquitectura Empresarial, Arquitectura de Seguridad, Arquitectura de Seguridad de la Información (ISA), Arquitectura de Seguridad de la Información Empresarial (EISA) y el Modelo de Arquitectura de Seguridad de la Información (MASI).

En el cuarto capítulo se presenta el diseño de una propuesta de arquitectura de seguridad para los datos personales con los que trabaja una empresa privada, la implementación de esta arquitectura tiene como finalidad principal cumplir con las disposiciones generales y dar cumplimiento satisfactorio a la Ley,sin interferir con las actividades cotidianas de la empresa.

Finalmente se presentan los anexos, que contiene los documentos de fundamentación legal de la Ley Federal de Datos Personales en Posesión de los Particulares, y los formatos necesarios para la implementación de la Arquitectura de Seguridad de Datos Personales de una Empresa Privada diseñada en el capítulo cuarto.

Pregunta de investigación

¿Es necesario que las organizaciones definan políticas y contraten a personal especializado en seguridad informática, para cumplir de manera satisfactoria con la Ley Federal de Protección de Datos Personales en Posesión de los Particulares?

Hipótesis

Si en la organización se definen políticas que atiendan la reglamentación gubernamental de seguridad de la información y se encarga su atención al área responsable de seguridad informática, se evitará la defraudación o violación de la Ley de Protección de Datos Personales en Posesión de los Particulares.

Objetivo general

Analizar la Ley federal de protección de datos personales en posesión de los particulares, para garantizar la implementación y cumplimiento de la misma mediante consideraciones en la seguridad de la información.

Objetivos específicos

- ✓ Conocer la ley federal de protección de datos personales en posesión de los particulares.
- ✓ Investigar la función de la seguridad informática.
- ✓ Analizar la conexión entre la ley de protección de datos personales y la seguridad informática.
- ✓ Diseñar una propuesta para el cumplimiento de la Ley Federal de protección de datos personales en posesión de los particulares.

Capítulo I. Antecedentes de la seguridad informática

1.1 Evolución de la informática

A simple vista la informática es una ciencia actual, sin embargo, tiene su propia historia que sería muy corta sí solo se considera como una serie de conocimientos tanto científicos como técnicos que sirven para tratar información de manera automática.

1.1.1 Antecedentes de la computadora

El principio real de las computadoras como las conocemos hoy en día, comienza con el trabajo de Charles Babbage en 1812, Babbage se dio cuenta de la relación natural que existe entre las máquinas y las matemáticas; las máquinas fueron las mejores en la realización de una tarea repetidas veces sin equivocarse, mientras las matemáticas requieren la repetición de unos pasos, Babbage propuso una máquina que realizaba diferentes ecuaciones esta máquina fue llamada "*Diference Engine*".

Después de 10 años de trabajo sobre el "*Diference Engine*", Babbage se inspiró y comenzó a trabajar en una computadora de utilidad general, que llamo "Máquina analítica", la cual incluyó mecanismos de entrada en forma de tarjetas perforadas con instrucciones para funcionar basado en la máquina para hacer telas de Jacquard, donde las tarjetas se colgaban sobre un tambor rotatorio de cuatro lados que permitía que se procesaran automáticamente, sin necesidad de intervención humana (Kidwell y Ceruzzi, 1994). Finalmente Babbage concluyó su máquina con una memoria para guardar más de mil números con hasta 50 dígitos decimales.

Después de haber sido satisfecha la necesidad del cálculo matemático, aparece otra necesidad alarmante, la de cómo tratar la enorme cantidad de información que empezaba a producirse en el mundo. El primer paso lo da Hermann Hollerith en 1880 considerado como el pionero del procesamiento automático de información que cien años después de la revolución francesa desarrollo la máquina de censos para poder procesar los datos que se referían a los censos poblacionales de los Estados Unidos de América, por medio de tarjetas perforadas.

Hollerith fue contratado por la Oficina de Censos de Estados Unidos para que preparara el análisis estadístico de los datos obtenidos en el censo de 1880. El trabajo duró siete años y medio y al final los volúmenes publicados tenían un gran número de errores, la tabulación manual y los resultados fueron inadecuados, sin embargo, Hollerith no desistió y concibió una máquina basada en la de Charles Babbage y utilizando el sistema de tarjetas perforadas de Jacquard (Coello, 2003).

La máquina estuvo lista en 1887 y utilizaba papel continuo en lugar de las tarjetas individuales, y así en el censo de 1890 el análisis de los datos se realizó en dos años y medio.

A partir de este momento empiezan a crearse máquinas de clasificación automática, tabuladoras y perforadoras de teclado, que serán como el disparo de salida de la carrera de esta naciente industria de procesadores (Coello, 2003).

Hollerith fundó en 1903 la *Tabulating Machine Company*, creando nuevas máquinas sobre variaciones de la primera y que se utilizaron para hacer un censo británico en 1911. En ese año se une con la *International Time RecordingCompany*, compañía dedicada a la fabricación de relojes, y con *Dayton ScaleCompany*, dando lugar ocho años más tarde a la *Computing TabulatingRecordingCompany*, de la que llego a ser presidente Thomas J. Watson en 1914 y que se transformó en la muy conocida IBM*International Business Machine Corporation*, en 1924 (Shurkin, 1996).

1.1.2 Generaciones de la computadora

Primera generación (1945-1956)

Al inicio de la Segunda Guerra mundial, los gobiernos buscaron la forma de desarrollar las computadoras y beneficiarse de su potencial estratégicamente. En 1941 el ingeniero Konrad Zuse desarrollo la computadora Z3 para diseñar aviones y misiles, en 1943 los británicos terminaron una computadora secreta, llamada Colossus, que podía descifrar códigos para leer los mensajes alemanes, Colossus no fue una computadora de uso general, fue únicamente diseñada para descifrar mensajes secretos; la existencia de la máquina fue guardada en secreto décadas después de la guerra.

El ingeniero Howard H. Ailen, quien era estudiante de Harvard y trabajador de IBM, logró crear una computadora electrónica en 1944, cuyo propósito fue crear diagramas balísticos para la marina de los Estados Unidos de Norte América, la calculadora automática para controlar secuencias de Harvard- IBM llevo por nombre Mark I y fue una computadora electrónica basada en el uso de interruptores (Coello, 2003).

Otro desarrollo de la computadora estimado por la guerra fue el Integrador Numérico Electrónico y Computadora (ENIAC) como resultado de los esfuerzos del gobierno de los Estados Unidos y la Universidad de Pensilvania, la computadora fue una enorme pieza de maquinaria con un consumo alto de energía, sus creadores fueron John Presper Eckert y John W. Mauchly en 1946, ENIAC fue una computadora de uso general con una velocidad mil veces más rápida que Mark I.

En el año 1945, John Von Neuman de la Universidad de Pensilvania, diseño la computadora EDVAC Computadora Electrónica Automática de Variables Discretas, la computadora tenía una memoria que le permitía guardar tanto el programa como los datos, esta técnica dio la posibilidad a detener la computadora en cualquier punto de trabajo y después reanudar; permitió mayor flexibilidad en la programación de la computadora. El elemento más importante en la arquitectura de Von Neuman fue la Unidad Central de Proceso que coordinaba todas las funciones de la computadora.

En 1951 fue construida la computadora UNIVAC Computadora Central Automática Universal de *Remington Rand*, esta computadora fue una de las primeras comerciales, los dueños de esta computadora fueron los dueños de la oficina del censo de los Estados Unidos y *General Electric*, uno de los éxitos de esta computadora fue el pronóstico sobre el ganador en las elecciones para la presidencia de Estados Unidos en 1952. Un año después las computadoras fueron equipadas con memorias magnéticas, que duplicaron la velocidad de procesamiento y la entrada de datos fue más rápida (Collins, 2000).

Segunda generación de computadoras (1956-1963)

Desde 1956 comenzaron a utilizar los transistores en las computadoras, junto con las memorias magnéticas, los transistores llevaron a ser más pequeñas, rápidas, seguras y eficientes. Las primeras supercomputadoras fueron, *Stretch*, fabricada por IBM y *Larc* fabricada por *Sperry Rand*ambas, estas computadoras pudieron manejar una enorme cantidad de datos, las máquinas eran caras y muy poderosas respecto a las necesidades de la mayoría de los negocios, por lo que su uso fue limitado.

La segunda generación de computadores remplazó el lenguaje máquina, permitiendo abreviar los códigos de programación y remplazarlos con los largos y difíciles códigos binarios (Coello, 2003).

Un ejemplo importante de esta generación es la computadora IBM 1401, que fue aceptada universalmente en la industria y fue considerada como uno de los modelos más importantes en la industria de las computadoras.

En 1964 la compañía IBM introduce el Sistema 360 que tuvo 6 procesadores y cuatro unidades periféricas, ese mismo año se desarrolló el lenguaje Basic como lenguaje de programación, para 1965 la mayor parte de la información financiera, que se utilizaba en operaciones de rutina estaba utilizando las computadoras de esta segunda generación.

El concepto de programa almacenado implicaba que las instrucciones que maneja la computadora, eran guardadas dentro de la memoria de la computadora y podrían ser reemplazadas rápidamente por un conjunto distinto de instrucciones con funciones diferentes.

La computadora podía ya imprimir facturas y minutos después diseñar productos o calcular sueldos, surgen lenguajes de programación más sofisticados y a un nivel más alto como COBOL y FORTRAN, estos lenguajes reemplazaron el código binario de las máquinas con palabras, oraciones y fórmulas matemáticas (Shurkin, 1996).

Tercera generación de computadoras (1964-1971)

En esta generación surge la utilización del cuarzo, en 1958 el ingeniero Jack Kilby de la compañía Texas Instruments, desarrolló el primer circuito integrado, el cual combinó tres componentes electrónicos en un pequeño disco de silicio que fue hecho de cuarzo.

Como resultado se incluyeron más componentes es un chip, lo que ha permitido crear sofisticadas computadoras del tamaño de un cuaderno, contenía una placa de circuitos integrados interconectados entre sí, incluyo el uso de un sistema operativo que permitió a las máquinas ejecutar varios programas diferentes al mismo tiempo gracias a un programa central que coordinaba la memoria de la computadora.

En 1965 Gordon Moore, el fundador de INTEL en 1968, pronosticó que el número de los transistores que componen a un chip se duplicaría cada año. En 1964 un chip de 2.5 m.m. contenía 10 componentes, para 1970 el chip ya tenía 1000 componentes, así que su comentario fue comprobado (Collins, 2000).

Cuarta generación (1971- 1981)

El adelanto de la cuarta generación fue disminuir las dimensiones y hacer circuitos integrados con gran escala de integración donde cientos de componentes fueron ajustados solo en un chip. En 1980 fue posible poner miles de componentes en un chip, el número de componentes ajustados en un chip aumentó con la tecnología de la integración de Ultra gran escala. Todo esto amplio la posibilidad de disminuir las dimensiones de la computadora y su precio, al tiempo que aumentó su poder, eficiencia y seguridad.

Las computadoras ya no fueron exclusivamente para los grandes negocios o para las oficinas y organismos del gobierno, a medida de la década de los 70los fabricantes buscaron llevar las computadoras hasta el consumidor en general, dando como resultado las computadoras personales fueron complementadas con paquetes de software y programas para uso cotidiano al mismo tiempo ofrecían muchas aplicaciones con mayor popularidad como la hoja de cálculo, entre otras aplicaciones.

Los pioneros en ofrecer las computadoras personales con estos servicios fueron *Apple Computers*, *Radio Shack* y *Commodore*, en los primeros meses del año 1980 se integran video juegos como *PacMan* y sistemas de video doméstico, aparece el lenguaje Pascal diseñado para programación estructural

En 1981 la compañía IBM fabricó su computadora personal con el procesador Intel 8088 y 64 KB de RAM para ser utilizada en la casa, oficina o escuela. Ese mismo año aparece el sistema operativo MS-DOS desarrollado por Microsoft.

Hasta nuestros días

En 1983 se desarrolla el lenguaje de programación Turbo Pascal, en 1990 dan a conocer el sistema operativo Windows 3.0, en 1985 Microsoft desarrolla MS-DOS donde comienza el interés por la interface gráfica de usuario (GUI), desde entonces las computadoras se hicieron cada vez más pequeñas y poderosas, y las interfaces de los sistemas operativos fueran más gráficas y llamativas dando como resultado las aplicaciones multimedia, música, video, sonido principalmente.

Se desarrollaron nuevos hardware y software que permiten la comunicación entre computadoras para formar una red y de esta manera compartir recursos como impresoras, scanner, el espacio de la memoria, el software, la información.

La comunicación entre sí puede ser mediante un cableado y de manera inalámbrica, el uso de las redes de comunicación es una de las herramientas más importantes y utilizadas en el mundo global, ya que nos permite acortar distancias y tiempos, no imaginamos la comunicación sin la Internet, el correo electrónico, las redes sociales entre otras ventajas que nos brindan las comunicaciones en nuestro ámbito laboral, escolar y social (Molina, 2005).

Las computadoras son una de las herramientas más versátiles que tenemos en la actualidad. Son capaces de simplificar y realizar nuestras tareas diarias, automatizar procesos tediosos, facilitan el intercambio de la información, entre otras.

Los sistemas de información nos permiten tener un control y organización de grandes cantidades de información así mismo poder compartirlas mediante el uso de Software y Hardware que son cada vez más sencillos de utilizar.

Surgen los Sistemas Expertos, que son aplicaciones informáticas que tienes como finalidad principal brindar información especializada al usuario sobre un área específica. El uso de este sistema debe de ser simple para que el usuario pueda interactuar con el sin ningún problema.

Los sistemas expertos son el producto de investigaciones en el campo de la inteligencia artificial ya que ésta no intenta sustituir a los expertos humanos, sino que se desea ayudarlos a realizar con más rapidez y eficacia todas las tareas que realizan (Sanders, 1995).

1.2 Evolución del concepto de seguridad

Según Borghello (2001) afirma que para entender el concepto de seguridad es necesario remontarse a la época primitiva, donde el hombre para evitar amenazas, reaccionaba con los mismos métodos defensivos que los animales: luchando y huyendo, para eliminar o evitar el daño, y afirma que desde entonces “nace la Seguridad Externa que es aquella que se preocupa por la amenaza de entes externos hacia la organización, y la Seguridad Interna que es aquella preocupada por las amenazas de nuestra organización con la organización misma; de estas dos se desprende la Seguridad Privada y Pública al aparecer el estado y depositar su confianza en unidades armadas”.

La Seguridad moderna se originó con la Revolución Industrial para combatir los delitos y movimientos laborales, tan comunes en aquella época, Henry Fayol en 1919 identifica la Seguridad como una de las funciones empresariales, luego de la técnica, comercial, financiera, contable y directiva.

Al definir el objeto de la Seguridad Gómez (1994) cita a Fayol quien dice: “…salvaguardar propiedades y personas contra el robo, fuego, inundación, contrarrestar huelgas y felonías, y de forma amplia todos los disturbios sociales que puedan poner en peligro el proceso e incluso la vida del negocio. Es, generalmente hablado, todas las medidas para conferir la requerida paz y tranquilidad (peace of Mind) al personal”.

Las medidas a las que se refiere Fayol, sólo se restringen a las exclusivamente físicas de la instalación, ya que el mayor activo era justamente ese: los equipos, ni siquiera el empleado. Con la aparición de los “cerebros electrónicos”, esta mentalidad se mantuvo, porque difícilmente alguien sería capaz, de atentar contra estos complicados aparatos como para poner en peligro la integridad de los datos por ellos utilizados.

Desde su nacimiento hasta la actualidad el concepto de seguridad es un concepto en continua revisión y con múltiples interpretaciones, sin embargo no ha perdido su esencial significado, que es salvaguardar, proteger contra robos, ataques, crímenes, espionajes o sabotajes. La seguridad implica la cualidad o estado de estar seguro, es decir evitar situaciones de exponerse al peligro, a la actuación para quedar a cubierto frente a contingencias adversas.

En la actualidad la seguridad, desde el punto de vista legislativo, está en manos de los gobernantes así como también existe el derecho informático y la informática jurídica, a quienes les toca decidir sobre su importancia, los delitos en que se puede incurrir, y el respectivo castigo o sanción correspondiente.

Este proceso ha conseguido importantes logros en las áreas de prevención del crimen, de los delitos informáticos, del terrorismo y riesgo más que en el pensamiento general sobre seguridad (Téllez, 2009).

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

En este proceso en donde se crea una relación entre la seguridad y las leyes, es importante la concientización del cumplimiento de las leyes para salvaguardar la paz en la sociedad.

1.3 Seguridad Informática

Debido al aumento en el uso de sistemas de información en todo el mundo ha ocasionado que exista la preocupación por la seguridad informática, que según Gutiérrez (2005) se refiere a la protección que necesita un sistema informático, el cual está formado por tres componentes fundamentales, el hardware, el software y datos, los cuales pueden sufrir algún tipo de daño y por lo tanto necesitan ser protegidos.

El hardware se encuentra compuesto por el conjunto de sistemas físicos, que constituyen la computadora como es: gabinete, *motherboard*, microprocesador, disco duro, unidades de almacenamiento extraíble, monitor, *mouse*, teclado, cables, instalaciones entre otros.

El software consiste en el conjunto de sistemas lógicos que hacen funcionar al hardware, como son sistemas operativos, paquetes, aplicaciones y programas.

La información, que en simples palabras es el conjunto de datos que pueden constituir registros, bases de datos, documentos y más.

El uso de los sistemas de información se ha extendido en ambientes comerciales, gubernamentales, militares e incluso en los hogares, Dando como consecuencia grandes cantidades de datos vitales y sensibles que se han confiado y almacenado cada vez más en computadoras.

En muchos de los casos las computadora contienen archivos y datos de configuración con contraseñas como pude ser de su correo electrónico, redes sociales o laborales, así como información que tiene un valor mayor en cual se incluye registros sobre individuos, negocios o algunas veces registros públicos y secretos gubernamentales o militares; así como también grandes transacciones monetarias que se realizan diariamente en forma de transferencia electrónica.

Según Firman (2005) un sistema seguro tiene que ser capaz de mantener las siguientes características fundamentales:

a) La confidencialidad es una característica donde sólo las personas autorizadas puede acceder al sistema, puede ser un recurso, un documento de texto, el disco duro, un servicio del sistema operativo y hasta nuestra propia computadora. La confiabilidad busca es que solo nosotros o quienes queremos, sean los únicos que lean ese archivo.

b) La integridad, consiste en asegurar que la modificación de un recurso sólo sea realizada por personas autorizadas, como por ejemplo un archivo de nuestra computadora solo puedes ser creado, modificado o borrado por nosotros mismos. Para asegurar la integridad de ese archivo.

c) La disponibilidad, implica que los recursos siempre tienen que estar a disposición de las personas autorizadas, un sistema tiene que estar funcionando continuamente para hacer que el recurso esté al alcance de quien esté autorizado a utilizarlo.

d) La autenticidad, son los métodos de autenticación para verificación de identidad puede clasificarse en tres categorías:

- Categoría 1: Algo que el usuario sabe. Un dato esencial, puede tratarse de algo de su persona o bien de un simple o complejo password.

- Categoría 2: Algo que el usuario lleva consigo. Puede ser un documento de identidad, una identificación, una tarjeta o cualquier otro elemento que uno lleva consigo.

- Categoría 3: Propiedad física o acto involuntario. La pupila, la voz y la huella dactilar, son ejemplos de propiedades físicas de un individuo y firmar es un acto involuntario, ya que uno no está pensando en hacer cada trazo, sino que los realiza en conjunto.

Existen múltiples ataques que se pueden presentar sobre los datos y romper con las características de un sistema seguro:

- Interrupción. Ataque contra la disponibilidad.

  Cuando los datos o la información de un sistema se ven corruptos, ya sea porque se han perdido, bloqueado o simplemente porque no están disponibles para su uso. Este tipo de ataque en la mayoría de las ocasiones no tiene mucha lógica por parte del atacante, salvo que se vea encerrado o perseguido.

- Intercepción. Ataque contra la confidencialidad.

  Lo que se logra es que un usuario no autorizado pueda acceder a un recurso y, por ende, la confidencialidad se vea divulgada.

- Fabricación. Ataque contra la autenticidad.

  Tiene lugar cuando un usuario malicioso consigue colocar un objeto en el sistema atacado. Este tipo de ataque puede llevarse a cabo con el objeto de hacer creer que ese archivo o paquete es el correcto o bien con la finalidad de agregar datos y obtener, de esta manera, un provecho propio.

- Modificación. Ataque contra la integridad.

  Puede contar o no con autorización para ingresar al sistema, manipula los datos de tal manera que la integridad se ve afectada por su accionar. Cambiar datos de archivos, modificar paquetes, alterar un programa o aplicación son sólo algunos ejemplos de este tipo de ataque.

Según el artículo publicado por Rayn (2011) en el manual de seguridad, la pérdida o uso inadecuado de la información nos puede perjudicar en diversas magnitudes como son:

1. El desperdicio de valiosas horas de trabajo.
2. El deterioro de la reputación o imagen de la empresa.
3. La pérdida de millones de pesos.
4. Aportar elementos para la planeación y realización exitosa de un delito.

Dentro de una empresa o institución es de gran importancia proteger la siguiente información: planes y estrategias de trabajo vitales para el buen funcionamiento de la empresa, los datos personales de los trabajadores así como de los clientes, de los proveedores, las campañas publicitarias y la información de proyectos presentes y futuros.

1.3.1 Vulnerabilidad

La mayoría de los sistemas tienen algún tipo de vulnerabilidad, esto no significa que el sistema sea defectuoso. El éxito de un ataque depende del grado de la vulnerabilidad, la fuerza del ataque y la efectividad de cualquier contramedida aplicada.

Las vulnerabilidades son el resultado de los errores de un software, o de fallos en el diseño del sistema, también pueden ser el resultado de las propias limitaciones tecnológicas.

1.3.1.1 Tipos de Vulnerabilidad

En el Cuadro 1 se explica cada uno de los tipos de vulnerabilidad:

Vulnerabilidad Física	Se presenta cuando existe una falla en las instalaciones de red, como es cableado desordenado, de mala calidad o que se encuentren expuestos. De igual forma se presenta cuando existe falta de control en el personal que tiene acceso a los sistemas.
Vulnerabilidad Natural	Se le llama así a los desastres naturales o sismos, a las inundaciones o incendios, cuando hay humedad o polvo excesivo o temperaturas que afecten a las maquinas donde se encuentran los sistemas.
Vulnerabilidad de Hardware	Puede ser cuando el hardware se encuentra defectuoso de fábrica o se le brinde un mantenimiento inadecuado, que dañe las computadoras.
Vulnerabilidad de Software	Es unos de los puntos más débiles porque puede permitir un acceso inadecuado a los sistemas de información. Es cuando existe una mala configuración e instalación de los programas o sistemas operativos e incluso la ejecución de virus por falta de actualizaciones al antivirus.

Vulnerabilidad del medio de almacenamiento	Se le llama si a la inadecuada utilización de los medios de almacenamiento, áreas o lugares de depósito inadecuado, mala calidad o uso de los medios genéricos.
Vulnerabilidad de comunicación	Este tipo de vulnerabilidad abarca todo el tránsito de la información, ya sea cableado, satélite, fibra, u ondas de radio inalámbricas.
Vulnerabilidad Humana	Son los daños que las personas puedan causar a la información, a los equipos o a los ambientes tecnológicos. De igual forma la falta de capacitación de los usuarios.

Cuadro 1. Tipos de vulnerabilidad (Creación propia).

1.3.3 Riesgo

La ISO 27001 (SGSI – Sistema de Gestión de seguridad de la información), define riesgo como "la probabilidad de que una amenaza se materialice, utilizando vulnerabilidades existentes de un activo o un grupo de activos, generándole pérdidas o daños."

En la definición anterior se pueden identificar varios elementos que se deben comprender adecuadamente para entender integralmente el concepto de riesgo. Estos elementos son: probabilidad, amenazas, vulnerabilidades, activos y pérdidas, ver Figura 1.

Figura 1Elementos del Riesgo (Lara, 2012).

En lo relacionado con seguridad, generalmente el riesgo se plantea solamente como amenaza, determinando el grado de exposición a la ocurrencia de una pérdida (por ejemplo el riesgo de perder datos debido a rotura de disco o virus informáticos).

1.3.2.1 Elementos del Riesgo

A continuación se describen cada uno de los elementos de riesgo que existen:

- **Probabilidad**

La probabilidad de ocurrencia de un riesgo puede realizarse de manera cuantitativa o cualitativa, siempre considerando que la medida no debe contemplar la existencia de ninguna acción favorable, es decir, debe considerarse en cada caso, las posibilidades que existen de que la amenaza se presente independientemente del hecho que sea o no contrarrestada.

- **Amenazas**

Las amenazas son aquellas acciones que ocasionan consecuencias negativas en la operativa de la organización, pueden ser las fallas o los ingresos no autorizados, los virus, el uso inadecuado de software, los desastres ambientales como: terremotos o inundaciones. Las amenazas pueden ser de carácter físico o lógico.

- **Vulnerabilidades**

Se refieren a las condiciones inherentes a los activos o presentes en su entorno, que favorecen para que las amenazas se materialicen a esto se llama actos vulnerables. El uso de las debilidades existentes es que las amenazas logran materializarse, es decir, las amenazas siempre están presentes, pero sin la identificación de una vulnerabilidad no podrán ocasionar ningún impacto.

- **Pérdidas**

Las pérdidas generadas pueden ser financieras, de corto plazo o de largo plazo. Se puede establecer que las más comunes son: la pérdida directa de dinero, la pérdida de confianza, la reducción de la eficiencia y la pérdida de oportunidades de negocio entre otras.

1.4 Objetivos de la Seguridad Informática

Entre los principales objetivos de la seguridad informática, propuestos por Gómez (2007), se destacan los siguientes:

- Minimizar o administrar riesgos, detectar posibles problemas y amenazas de seguridad dentro de la organización.
- Garantizar el uso adecuado de los recursos y de las aplicaciones del sistema.
- Limitar las pérdidas y conseguir la adecuada recuperación del sistema en caso de un incidente de seguridad.
- Cumplir con las regulaciones vigentes y con el marco legal.

1.5 Razones para Implementar la Seguridad de la Información.

- Para permitir el correcto funcionamiento de la actividad empresarial,
- Es una obligación legal normativa en México para dependencias de gobierno que manejen información personal. Lo anterior de acuerdo a Ley Orgánica de Protección de Datos de Carácter Personal (LOPD), (6 de julio de 2010) y Ley de Servicios de la Sociedad de la Información (LSSI) en 2002,
- Puede actuar de factor diferenciador (certificación ISO 17799 o ISO 27002), es un estándar para la seguridad de la información,
- Protege ante posibles fallos humanos, intencionales o no,

- Evita que usuarios internos puedan atacar sistemas externos (con la responsabilidad legal que ello conlleva),
- Previene la entrada de intrusos en los sistemas,
- Impide que usuarios descontentos puedan causar daños importantes que lleguen a alterar o incluso a detener las actividades de la organización.

Capítulo II Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) en México

2.1 Razones para implementar la seguridad de la información en México

Para poder entender la situación que enfrenta México, a nivel de seguridad informática es importante realizar un análisis de las Fortalezas, Oportunidades Debilidades y Amenazas (FODA) que se muestra en el Cuadro 2.

Fortalezas	Oportunidades
- Existe una mayor preocupación por la seguridad de la información en las empresas grandes en México. - Las organizaciones en México ponen más atención en la implementación de políticas de seguridad informática. - Se cuenta con una legislación que vigila el uso de los datos personales. - El IFAI es el encargado de dar seguimiento y solución a las demandas por mal uso de los datos personales.	- Nivel alto se Seguridad Informática en comparación a la mayoría de países latinoamericanos. - México cuenta con una legislación informática, contra delitos informáticos. - La creación de leyes para la protección de información sensible tomando en cuenta organismos internacionales.

Debilidades	Amenazas
- Solo las empresas grandes, tienen mayor conciencia respecto al valor de la información. - Las microempresas no cuentan con un presupuesto para implementar políticas de seguridad informática. - Falta de capacitación para los empleados o directivos de las empresas. - Falta de presupuesto para investigaciones tecnológicas.	- México se encuentra renuente en adoptar nuevas tecnologías. - Tenemos un nivel muy por debajo de los países desarrollados. - La creación de nuevas tecnologías, que muchas veces tarda en llegar a México.

Cuadro 2. Análisis de fortalezas, oportunidades, debilidades y amenazas de la seguridad informática en México (Creación propia).

La seguridad informática en México actualmente adquiriere gran importancia, y el nivel de conciencia que se tiene en las empresas mexicanas aumenta día con día y aumenta el grado de conocimiento que se tiene en los diferentes ámbitos de la seguridad informática: como es seguridad física, seguridad frente agresores externos y seguridad frente agresores internos, así como la identificación de elementos relacionados con la seguridad informática considerados importante por los responsables de su implementación dentro de las organizaciones.

De acuerdo con Espinoza (2009), México se encuentra en un nivel intermedio o incluso superior al de la mayoría de países latinoamericanos, pero en un nivel muy por debajo de los países desarrollados.

Siguiendo a Espinoza, en México las organizaciones grandes, tienen una mayor conciencia respecto al valor de su información, así como también de la responsabilidad que se adquiere al manejar información de terceros y se esfuerzan por difundir una cultura sobre el tema al interior de sus organizaciones. De la misma manera estas organizaciones cuentan con un presupuesto mayor y mejor estructurado.

Dentro de sus principales rezagos se encuentra que existe una cultura de seguridad poco extendida, falta de capacitación tanto de los responsables de la seguridad de la información a nivel interno, como de algunos proveedores de soluciones relacionadas, así como un bajo nivel de conciencia entre directivos de las organizaciones, carencia de foros y de presupuesto para incentivar las investigaciones tecnológicas.

México en general esta renuente a adoptar de forma inmediata nuevas tecnologías en seguridad informática, esto derivado al rechazo a utilizarlas en el momento en que son puestas al mercado.

La capacitación en materia de la seguridad informática es uno de los retos a enfrentar en México, no solo a promover un mayor conocimiento por parte de los usuarios, sino también de los especialistas del ramo quienes tienen que adaptarse con rapidez a la dinámica de reglas a nivel internacional, nacional y local, así como a la nueva tecnología.

El problema de Seguridad de la información en México tiene que ver con los avances en la implementación de un buen sistema de gestión de riesgo lo cual ha tomado relevancia en los últimos 15 años, muchas empresas están buscando definir su estrategia de seguridad de la información con un alcance no solo pequeño ni incipiente, con el interés de ir avanzando en la madurez del proceso de administración de riesgo.

La investigación de Espinoza (2009), concluye que México está teniendo avances importantes en atención a la seguridad de la información y que las empresas de todo tipo están dando mayor importancia al tema de la seguridad de la información.

Un individuo va dejando información personal, en escuelas, bancos, comercios, empresas donde labora, o simplemente en encuestas que muchas veces no sabemos si esos datos son utilizados correctamente y vigilados hasta su destrucción.

Por esa razón México se ha puesto manos a la obra para crear una legislación dedicada a vigilar y salvaguardar la integridad de cada uno de los individuos que habitamos este país.

Lo importante sería que los ciudadanos y autoridades acepten que las necesidades globales y el uso creciente de las tecnologías nos exigen un control sobre delitos informáticos que son cada vez más frecuentes.

2.2 Surgimiento de la Ley Federal de Datos Personales en Posesión de los Particulares en México

Como consecuencia del gran despliegue tecnológico, actualmente es importante contar con una legislación que proteja los datos personales, los riesgos tecnológicos son un asunto de todos los días para los ejecutivos de las organizaciones privadas e instituciones gubernamentales, las amenazas a la confidencialidad son una preocupación constante que crece ala par del avance tecnológico.

En el capítulo anterior se menciona, el uso excesivo de las tecnologías de la información y las telecomunicaciones, ha ocasionado que los datos personales sean utilizados para fines distintos para los que originalmente fueron recabados, de esta manera son transmitidos a instancias distintas a las que el dueño de los datos confió dicha información.

En México la preocupación por la protección de la información de los particulares es de fundamental interés, ya que es considerado un problema globalizado, para controlar esta situación se dio a conocer la creación de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, que fue publicada en el mes de Julio del año 2010 en el Diario Oficial de la Federación (DOF, 05/07/2010),para comprender esta ley es importante conocer los antecedentes que dieron lugar a su publicación.

Los primeros antecedentes surgen en Europa, con la Resolución 509 de la Asamblea del Consejo de Europa sobre los derechos humanos y nuevos logros tecnológicos emitida en 1967, sin embargo, fue hasta la década de los setenta cuando Alemania, Francia, Dinamarca, Austria y Luxemburgo aprobaron leyes nacionales para la protección de datos personales (Arenas, 2006).

Con la invención de la computadora personal, el Consejo de Europa promulga el convenio No. 108 con el propósito de proteger a las personas frente al tratamiento de sus datos. Posteriormente en el 2000 se aprobó la Carta de Derechos Fundamentales de la Unión Europea, en la que se jerarquizó la protección de datos personales al rango de derechos fundamentales.

El Convenio 108 consta de 27 artículos agrupados en 7 capítulos y los puntos más relevantes que conforman el convenio son:

- Artículo 4. Cada parte tomará las medidas necesarias para la protección de datos comenzando en el momento mismo de la entrada en vigor del convenio.
- Artículo 5. Los datos personales a proteger deberán ser obtenidos de manera leal, legítima y se registrará un fin o uso leal y legítimo. Además, deberán ser actualizados.
- Artículo 6. Se categorizan los datos y solamente se podrán tratar en medios automatizados bajo garantías de seguridad apropiadas: datos que revelen origen racial, opiniones políticas, convicciones religiosas u otras, datos de salud, de vida sexual y condenas penales.
- Artículo 8. Toda persona registrada deberá tener conocimiento de la existencia de esa base de datos y además podrá saber la finalidad de esos registros. Adicionalmente, podrá rectificar o ratificar datos, así como solicitar el borrado de su registro.
- Artículos 18 y 19. Creación de un Comité Consultivo para toma de decisiones, propuestas de enmiendas y aplicación del convenio.

Por otra parte, en 1980 la Organización para la Cooperación y el Desarrollo Económico la (OCDE), emitió una recomendación que contiene las directrices relativas a la protección de la privacidad y flujos transfronterizos de datos personales (Troncoso, 2010), que constituyó el primer instrumento internacional que analiza a profundidad el derecho a la protección de estos datos.

La OCDE invita a los países que la integran a poner mayor interés en materia de regulación a la protección de datos personales, en vista de la inexistencia de una regulación uniforme en esta materia en el Foro de Cooperación Económica Asia Pacífico la (APEC), en ese mismo año se estableció un Grupo de Manejo de Comercio Electrónico que tiene dentro de sus principales actividades el desarrollo de legislaciones y políticas compatibles entre las economías participantes en el campo de la privacidad.

Por ello, APEC ha emitido lineamientos generales en la protección de datos personales, con el propósito de establecer cuerpos legales correspondientes para lograr un flujo de datos seguros, pero al mismo tiempo, sin obstáculos para el fomento del comercio.

En 1990 la Organización de las Naciones Unidas (ONU), emitió la Resolución 45/95 que contiene una lista básica de principios para la protección de datos personales de aplicación mundial, como la de exactitud de los mismos, la determinación de su finalidad, su acceso y la no discriminación (Ortega, 2008).

El desarrollo normativo en el ámbito internacional ha buscado proteger a la persona y no al dato (que de cualquier forma la intensión sigue siendo proteger a las personas). Estas disposiciones establecen los principios y derechos que tiene un individuo para exigirle tanto al estado como a los particulares quién, cuándo y para qué, pueden utilizar sus datos personales. Los ejes rectores pueden resumirse en el principio de licitud y trato leal de los datos, de finalidad, de proporcionalidad, de calidad y de seguridad.

En el 2008 la Cumbre Mundial de la Seguridad de la Sociedad de la Información, hizo un llamado para pedir “normas mundiales sobre la privacidad de la información, convocando a todas las partes interesadas en garantizar el respeto a la privacidad y a la protección de información y datos personales, ya sea mediante la adopción de una legislación, la aplicación de marcos de colaboración, de mejores prácticas y medidas tecnológicas y de autorregulación por parte de empresas y usuarios" (Civitas, 2006).

En el artículo publicado por Sánchez y Rojas en 2012, mencionan que en el tema de la protección de datos, el mundo se rige principalmente por dos vertientes.

a) El modelo europeo el cual busca proteger la información y la propiedad de la misma, conservando la honorabilidad de la persona aun cuando éste hubiese fallecido, y se basa principalmente en los derechos humanos de los individuos.
b) El modelo estadounidense que pretende proteger la información de las personas con el concepto de derecho a la privacidad, el cual puede extinguirse con la muerte del sujeto, este modelo se deriva de motivos comerciales ya que las empresas utilizaban de manera indiscriminada esa información.

Para comprender la diferencia que existe entre un modelo y otro, se presenta un cuadro comparativo de los modelos (véase Cuadro 3).

Modelo Europeo (protección de datos)	Modelo americano (privacidad)
Enfoque preventivo	Todo se resuelve en las cortes
Socialmente Orientado	Enfoque individual
Confianza en el gobierno (cohesión y salvaguardias)	Confianza en el mercado (enfoque de negocios)
Los datos se recaban cuando es necesario	Los datos se recaban cuando es conveniente
Los derechos y las excepciones se prevén en Ley	Los alcances jurídicos se resuelven caso por caso en las cortes

Modelo Europeo (protección de datos)	Modelo americano (privacidad)
Existen autoridades especializadas e independientes	No existe autoridades concretas, sino algunas sectoriales
Se protege a todo individuo que esté en territorio europeo	No se protege a ciudadanos no estadounidenses

Cuadro 3. Comparativo de modelos de marcos legislativos de Ley de Protección de Datos (Creación propia).

En el Cuadro 4 se presenta un listado de los países que cuentan con una ley especial para la protección de datos personales son los siguientes:

Países	Leyes de protección de datos personales
Alemania	En 1970 fue aprobada la primera ley de protección de datos (Daten Schutz). En 1977 El Parlamento Federal Alemán aprueba la Ley Federal Bundesdatenschutzgesetz. Estas leyes impiden la transmisión de cualquier dato personal sin la autorización de la persona interesada.
Suecia	En 1973 entra en vigor la primera ley en el mundo para la protección de la información de particulares. Esta ley cuenta con un organismo supervisor para su cumplimiento llamado *Data InspektionBoard.*
Estados Unidos de Norteamérica	La protección de datos tiene base en la *PrivacyAct* de 1974. Que tiene como finalidad expandir las capacidades de la ley estadounidense para combatir el tráfico de contenidos con derechos de autor y bienes falsificados a través de Internet, es por ello que su principal función es la protección de los datos en el comercio electrónico.

Unión Europea	El primer convenio internacional de protección de datos fue firmado en 1981por Alemania, Francia, Dinamarca, Austria y Luxemburgo. Es conocida como “Convenio 108” que consta de 27 artículos agrupados en 7 capítulos y su objeto es garantizar el respeto de los derechos y libertades fundamentales de toda persona física, sin importar su nacionalidad, con respecto al trato automatizado de sus datos, sensibles o comunes, ya sea en el sector público o privado.
España	La Ley Orgánica 15 de 1999, establece la Protección de Datos de Carácter Personal. Esta Ley ha sido importante para Latinoamérica porque se ha utilizado como firme referencia del modelo europeo.
Latinoamérica	En América Latina, las leyes de protección de datos personales surgen como una necesidad derivada del incremento del uso de las tecnologías de la información y el aumento de las vulnerabilidades asociadas. En su mayoría, estas leyes se asemejan el modelo europeo: En Argentina la Lay 25.326 (2000), Chile (1999), Panamá (2002), Brasil (1997), Paraguay (2000) y Uruguay (2008).
Rusia	En el año 2006 fue aprobada una exhaustiva Ley de Protección de Datos Personales, sin embargo, actualmente, se encuentra en proceso de modificación a su ley federal de protección de datos de 2006, el propósito es mejorar algunos aspectos de seguridad. Uno de los cambios indica que el reglamento establecerá los requisitos de seguridad para el procesamiento de datos biométricos.

Perú	La ley 29.733 del 2 de julio de 2011 es una de las más nuevas en el mundo. Que se refiere a la protección de datos personales y señala en su artículo 2º que los datos biométricos son datos personales sensibles.
México	Publica en 5 de Julio de 2010 en el Diario Oficial, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

Cuadro 4. Leyes de Protección de Datos en el mundo (Creación propia).

En México, el debate alrededor de este tema inició en el año 2001, cuando se presentó la primera iniciativa de ley en materia de protección datos personales. A lo largo de ese tiempo fueron presentadas 8 iniciativas, cuyas propuestas oscilaron entre el modelo garantista, que entorpece el libre flujo de datos, y el modelo liberalizado, que no plantea puntos mínimos regulatorios para dar certeza al ciudadano; por lo que ninguna de ellas prosperó.

Fue hasta el mes de abril de 2009 que la Comisión de Gobernación de la Cámara de Diputados de la LX Legislatura, aprobó un dictamen de la ley, mismo que por razones ajenas al ámbito parlamentario (la epidemia de influenza), no logró ser discutido en el Pleno. Sin embargo, al inicio de los trabajos de la LXI Legislatura, la Comisión de Gobernación reabrió el debate.

Convencidos de la relevancia del tema, los miembros del Congreso de la Unión y el Presidente de la República Mexicana el Lic. Felipe de Jesús Calderón Hinojosa, aprobaron la Ley Federal de Protección de Datos Personales en Posesión de los Particulares el 27 de abril de 2010. Una legislación moderna que coloca a nuestro país entre los regímenes que protegen este tipo de derechos propios de las democracias en el mundo.

El 5 de Julio de 2010, el Presidente de la República Mexicana da a conocer en el Diario Oficial de la Federación, que el Honorable Congreso de la Unión dirige el siguiente decreto:

"EL CONGRESO GENERAL DE LOS ESTADOS UNIDOS MEXICANOS, DECRETA:

SE EXPIDE LA LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LOS PARTICULARES Y SE REFORMAN LOS ARTÍCULOS 3, FRACCIONES II Y VII, Y 33, ASÍ COMO LA DENOMINACIÓN DEL CAPÍTULO II, DEL TÍTULO SEGUNDO, DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA GUBERNAMENTAL.(DOF:05/07/2010)

Esta Ley (Anexo 1) regula la forma y condiciones en que deben utilizarse los datos personales por parte de personas físicas o morales en el ámbito privado. Tiene como objetivo garantizar la protección de la información personal y que puedan ejercer el derecho a decidir, de manera libre e informada, sobre el uso que los entes privados darán a los datos. A esto se le conoce como **"autodeterminación informativa".**

2.3 Disposiciones generales de Ley Federal de Protección de Datos Personales en Posesión de los Particulares

Esta ley es federal y de orden público, además tiene aplicación en todo el territorio mexicano, su finalidad es la protección de los datos personales en posesión de los particulares, regular su tratamiento legítimo para garantizar el derecho a la autodeterminación informativa de las personas.

2.3.1 Datos personales, sensibles y biométricos

Los **datos personales** son aquellos datos que brindan información acerca de un individuo como son: nombre, teléfono, domicilio, fotografía, huellas dactilares, así como cualquier otro dato que pueda identificar al individuo.

Existen diferentes categorías de datos, los cuales se presentan a continuación:

Categoría	Ejemplos
Identificación	✓ Nombre ✓ Domicilio ✓ Teléfono ✓ Correo Electrónico ✓ Firma ✓ RFC ✓ CURP ✓ Fecha de Nacimiento ✓ Estado Civil
Laborales	✓ Puesto ✓ Domicilio ✓ Correo electrónico del trabajo ✓ Teléfono del trabajo
Patrimoniales	✓ Información Fiscal ✓ Historial Crediticio ✓ Cuentas bancarias ✓ Ingresos y Egresos
Académica	✓ Trayectoria Educativa ✓ Título ✓ Número de cédula ✓ Certificados
Ideológicas	✓ Creencia Religiosa ✓ Afiliación política o sindical ✓ Pertenencia a organizaciones civiles o religiosas
Salud	✓ Estado de Salud ✓ Historial clínico ✓ Enfermedades ✓ Información psicológica o psiquiátrica

Características Personales	✓ Tipo de sangre ✓ ADN ✓ Huella Digital
Características Físicas	✓ Color de piel ✓ Iris o cabello ✓ Señas Particulares
Vida	✓ Hábitos sexuales
Origen	✓ Étnico y racial

Cuadro 5. Categorías de los datos personales (Creación propia).

Los **datos personales sensibles** son aquellos que requieren especial protección, ya que se refieren a información que puede revelar aspectos íntimos de una persona como: origen racial o étnico, estado de salud presente y futura, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual; que afectan la esfera más íntima de la persona y cuyo uso indebido, puede ser causa de discriminación o bien ponerlo engrave riesgo.

Sánchez Pérez y Rojas González (2012), mencionan la existencia de los **datos biométricos**. Que son aquellos rasgos físicos, biológicos o de comportamiento de un individuo que lo identifican como único del resto de la población. Aquellos sistemas informáticos en los que se mide algún dato biométrico, como parte del proceso de identificación o autentificación de un sujeto, son conocidos como sistemas de seguridad biométrica o simplemente sistemas biométricos.

La siguiente lista son algunos ejemplos de datos biométricos:

- Huellas dactilares
- Geometría de la mano
- Análisis del iris
- Análisis de retina
- Venas del dorso de la mano

- Rasgos faciales
- Patrón de voz
- Firma manuscrita
- Dinámica de tecleo
- Cadencia del paso al caminar
- Análisis gestual
- Análisis del ADN

2.3.2 Principios rectores de la Protección de Datos Personales

En el reglamento de la LFPDPPP (Anexo 2) se define a los principios de protección de datos como una serie de reglas mínimas, que deben observar las empresas o entes privados que tratan datos personales, garantizando con ello un uso adecuado de la información personal, dichos principios se explican en el siguiente cuadro 6 (DOF: 21/12/2011).

PRINCIPIOS RECTORES DE LA PROTECCIÓN DE DATOS PERSONALES	DEFINICIÓN
PRINCIPIO DE LICITUD	Es el compromiso que deben asumir los entes privados, que tratan la información cuando solicitan la prestación de un bien o servicio, respetando en todo momento la confianza que depositan en ellos los individuos, para el buen uso que le darán a los datos.

PRINCIPIO DE CONSENTIMIENTO	Al ser dueño de los datos, este principio permite decidir de manera informada, libre, inequívoca y especifica si desean compartir su información con otras personas. Implica que las empresas privadas deben solicitar la autorización para poder tratar la información que les concierne.
PRINCIPIO DE CALIDAD	Los datos en posesión de las empresas privadas, deben estar actualizados y reflejar con la veracidad de la información.
PRINCIPIO DE INFORMACIÓN	Se refiere a la potestad que le otorga la ley a los particulares, de conocer previamente las características esenciales del tratamiento a los que serán sometidos los datos personales que se proporcionen a las empresas privadas.
PRINCIPIO DE PROPORCIONALIDAD	Las empresas solo podrán recabar los datos estrictamente necesarios e indispensables para la finalidad que se persigue y que justifica su tratamiento.
PRINCIPIO DE RESPONSABILIDAD	Quienes tratan datos personales deben asegurar que ya sea dentro o fuera de nuestro país, se cumplan con los principios esenciales de protección de datos personales, comprometiéndose a velar siempre por el cumplimiento de estos principios.

Cuadro 6. Principios rectores de la protección de datos personales (Creación propia).

2.3.3 Aviso de Privacidad

Para el cumplimiento de la LFPDPPP las personas físicas o morales de carácter privado deben contar con un Aviso de Privacidad, que es un documento que debe ponerse a disposición de los titulares, a través de formatos impresos, digitales, visuales, sonoros o en cualquier otra tecnología.

El Aviso de Privacidad deberá contener al menos, la siguiente información:

I. La identidad y dominio del responsable que recaba los datos.
II. Las finalidades del tratamiento de los datos.
III. Las opciones y medios que el responsable ofrezca a los titulares para limitar el uso y divulgación de los datos.
IV. Los medios para ejercer los derechos de acceso, rectificación, cancelación u oposición de acceso, rectificación, cancelación y oposición, de conformidad con lo dispuesto en esta ley.
V. Explicar las transferencias de datos, si es que ocurren.
VI. Y explicar 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 la LFPDPPP (DOF:05/07/2010).

2.3.4 Derechos de Acceso, Rectificación, Cancelación y Oposición (ARCO)

El derecho a la protección de los datos es la facultad que otorga la Ley para que un individuo, como dueño de los datos personales, decida a quién proporciona su información, cómo y para qué; este derecho permite acceder, rectificar, cancelar y oponerse al tratamiento de su información personal, algunas veces el dueño de los datos no tiene oportunidad de realizar estos derechos a lo cual se puede auxiliar de un representante legal, que se encargara de realizar todos los trámites necesarios para llevar a cabo estos derechos. Por sus iníciales, son conocidos comúnmente como derechos ARCO.

Para llevar a cabo los derechos ARCO es necesario basarnos en el reglamento de la LFPDPPP se dio a conocer en el DOF, el 21 de diciembre de 2011 (Tercera Sección) en el se explica cada uno de los derechos a los que el individuo puede recurrir en caso de necesitar hacer cumplir esta ley.

2.3.4.1 Derecho de Acceso

Cada uno de los titulares de los datos personales o algunas veces un representante legal puede solicitar a una determinada empresa que informe si en sus bases de datos tiene algunos de sus datos personales. Para ejercer este derecho se debe presentar a la empresa una solicitud, puede ser escrita o por medio electrónico.

Según el Reglamento de LFPDPPP estos son los artículos para el derecho de acceso:

Artículo 101. El titular, en términos de los dispuestos por el artículo 23 de la Ley, tiene derecho a obtener del responsable sus datos personales, así como información relativa a las condiciones y generalidades del tratamiento.

Artículo 102. La obligación de acceso se dará por cumplida cuando el responsable ponga a disposición del titular los datos personales en el sitio, respetando el periodo señalado en el artículo 99 del reglamento de la LFPDPPP, o bien mediante la expedición de copias simples, medios magnéticos, óptico, sonoros, visuales u holográfico, o utilizando otras tecnologías de la información que se hayan previsto en el aviso de privacidad. en todos los casos, el acceso deberá ser en formatos legibles o comprensibles para el titular.

Cuando el responsable así lo considere conveniente, podrá acordar con el titular medios de reproducción de la información distintos a los informados en el Aviso de Privacidad.

Se debe presentar una solicitud que contenga los siguientes datos: nombre, domicilio o medio para recibir información, en caso de un representante legal debe incluir documentación que acredite a la persona, del mismo modo explicar cuáles son los datos a los que se quiere tener acceso, así como otro elemento que facilite la localización de sus datos personales.

Es importante conservar la constancia de solicitud que fue presentada pues si no se obtiene respuesta o no quedas satisfecho puedes acudir al Instituto Federal, de Acceso a la Información Pública y Protección de Datos (IFAI).

2.3.4.2 Derecho de Rectificación

La rectificación es un derecho que otorga la ley a que se corrijan los datos personales que una empresa tenga en sus bases, aplica cuando los datos son incorrectos, imprecisos, incompletos o desactualizados.

Los artículos que se deben tomar en cuenta son los siguientes:

Artículo 103. De conformidad con lo dispuesto por el artículo 24 de la ley, el titular podrá solicitar en todo momento al responsable que rectifique sus datos personales que resulten ser inexactos o incompletos.

Artículos 104. La solicitud de rectificación deberá indicar a qué datos personales se refiere, así como la corrección que haya de realizarse y deberá indicar la documentación que ampare la procedencia de los solicitado. El responsable podrá ofrecer mecanismos que faciliten el ejercicio de este derecho en beneficio del titular.

Se debe presentar una solicitud que contenga los siguientes datos: nombre, domicilio o medio para recibir información, en caso de un representante legan debe incluir documentación que acredite a la persona, especificar los datos que se desean rectifica, así como algún documento que justifica esta acción.

Se debe anexar cualquier documento que facilite la localización de los datos y el interesado deberá conservar la constancia de solicitud pues será necesaria en caso de acudir al IFAI.

2.3.4.3 Derecho de Cancelación

Es la facultad que le otorga la ley para que el interesado solicite la cancelación de sus datos personales de las bases de datos de una determinada empresa, la cual debe de dejar de tratar los datos, en especial cuando el tratamiento no cumpla con las disposiciones legales aplicables.

Los datos deberán ser bloqueados y posteriormente suprimidos de las bases de datos, esta solicitud procede cuando la información personal ya no es necesaria para las actividades de la empresa.

Los artículos del reglamento de la LFPDPPP que se deben cumplir son los siguientes:

Artículo 105. En términos del artículo 25 de la Ley, la cancelación implica el cese en el tratamiento por parte del responsable, a partir de un bloque de los mismos y su posterior supresión.

Artículo 106. El titular podrá solicitar en todo momento al responsable la cancelación de los datos personales cuando considere que los mismos no están siendo tratados conforme a los principios y deberes que establece la ley y el reglamento.

La cancelación procederá respecto de la totalidad de los datos personales del titular, contenidos en una base de datos, o sólo parte de ellos, según lo haya solicitado.

Artículo 107. De resultar procedente la cancelación, y sin perjuicios de lo establecido en el artículo 32 de la Ley, el responsable deberá:

I. Establecer un periodo de bloqueo con el único propósito de determinar posibles responsabilidades en relación con su tratamiento hasta el plazo de prescripción legal o contractual de éstas, y notificarlo al titular o a su representante en la respuesta a la solicitud de cancelación, que se emite dentro del plazo de veinte días que establece el artículo 32 de la Ley.
II. Atender las medidas de seguridad adecuadas para el bloqueo;
III. Llevar a cabo el bloqueo en el plazo de quince días establece el artículo 32 de la Ley, y
IV. Transcurrido el periodo de bloqueo, llevar a cabo la supresión correspondiente, bajo las medidas de seguridad previamente establecidas por el responsable.

Artículo 108. En términos del artículo 3, fracción III de la Ley, el bloqueo tiene como propósito impedir el tratamiento, a excepción del almacenamiento, o posible acceso por persona alguna, salvo que alguna disposición legal prevea lo contrario.

El periodo de bloqueo será hasta el plazo de prescripción legal o contractual correspondiente.

La petición se deberá presentar por escrito, por medios electrónicos, ópticos o de cualquier otra tecnología; deberá contener: el nombre y domicilio o medio para recibir información, identificación o documentos que acrediten la personalidad del representante legal, especificar los datos que deben ser cancelados así como cualquier otro elemento o documento que facilite la localización de los datos personales, de ser posible, la finalidad del tratamiento para la cual son tratados tus datos personales.

De igual forma que en los otros derechos es importante conservar la constancia de la solicitud que se ha presentado a la empresa que tiene sus datos ya que es indispensable para solicitar el apoyo del IFAI.

2.3.4.4 Derecho de Oposición

Consiste en el derecho que tienen las personas para solicitar a una empresa privada que pretende realizar el tratamiento de los datos personales, que se abstenga de hacerlo en determinadas situaciones, por ejemplo, para fines publicitarios. La solicitud deberá contener nombre, domicilio o medio para recibir información sobre el tema, la identificación del representante legal en caso de ser necesario y especificar las razones por las cuales se opone al tratamiento.

Los artículos que regulan la oposición son los siguientes:

Artículo 109. En términos del artículo 27 de la Ley, el titular podrá, en todo momento, oponerse al tratamiento de sus datos personales o exigir que se cese en el mismo cuando:

I. Exista causa legítima y su situación específica así lo requiera, lo cual debe justificar que aun siendo lícito el tratamiento, el mismo debe cesar para evitar que su persistencia cause un perjuicio al titular, o
II. Requiera manifestar su oposición para el tratamiento de sus datos personales a fin de que no se lleve a cabo el tratamiento para fines específicos.

No procederá el ejercicio del derecho de oposición en aquellos casos en los que el tratamiento sea necesario para el cumplimiento de una obligación legal impuesta el responsable.

Artículo 110. Para el ejercicio del derecho de oposición, los responsables podrán gestionar listas de exclusión propios en los que incluyan los datos de las personas que han manifestado su negativa para que trate sus datos personales, ya sea para sus productos o de terceras personas.

Asimismo, los responsables podrán gestionar listados comunes de exclusión por sectores o generales.

En ambos casos, la inscripción del titular a dichos listados deberá ser gratuita y obligar al titular una constancia de su inscripción al mismo, a través de los mecanismos que el responsable determine.

Artículo 111. El Registro público de consumidores previsto en la Ley Federal de Protección al Consumidor y el Registro Público de Usuarios previsto en la Ley de Protección y Defensa al Usuario de Servicios Financieros, continuarán vigentes y se regirán de conformidad con lo que establezcan las leyes en cita y las disposiciones aplicables que de ellas derivan.

2.3.5 El Instituto Federal de Acceso a la Información y Protección de Datos (IFAI) encargado del cumplimiento de la LFPDPPP

El IFAI es la autoridad garante en materia de protección de datos personales, la Ley le ha otorgado la facultad de difundir el conocimiento de este nuevo derecho entre la sociedad mexicana, de promover su ejercicio y vigilar su debida observancia por parte de los entes privados que posean datos personales.

El Instituto podrá llevar a cabo inspecciones a los sistemas de bases de datos de las empresas a fin de corroborar el debido cumplimiento de las disposiciones contenidas en la Ley.

Si no estás satisfecho con lo que la empresa te respondió al ejercer tu derecho de acceso, rectificación, cancelación u oposición, o bien, no obtuviste respuesta, puedes acudir al IFAI. Mediante un procedimiento sencillo y expedito, el Instituto atenderá tu solicitud y vigilara el proceso hasta llegar al fin.

Con el propósito de coadyuvar con el Instituto en la debida aplicación de la Ley, dependencias de la Administración Pública Federal colaborarán con el IFAI en la emisión de la regulación que corresponda. Entre ellas están las secretarías de Economía, Salud, Comunicaciones y Transportes, Hacienda y Crédito Público y Educación, las cuales deberán emitir normas específicas para la protección de los datos personales en los sectores económico, de salud, telecomunicaciones, financiero y educativo.

2.3.6 Sanciones a los que no cumplan la LFPDPPP satisfactoriamente

El IFAI, en su carácter de autoridad garante, tiene la facultad de imponer sanciones a aquellas empresas que no cumplan alguna disposición de la Ley.

A continuación se mencionan algunas de las posibles sanciones:

I. Advertencia

II. Multa de 100 a 160,000 días de salario mínimo vigente en el Distrito Federal, cuando la empresa actúe con negligencia o dolo con respecto a la información personal, no observe los principios de protección de datos establecidos en la Ley u omita datos en el Aviso de Privacidad

III. Multa de 200 a 320,000 días de salario mínimo general vigente en el Distrito Federal, cuando incumpla con su deber de confidencialidad en el tratamiento de los datos, cambie la finalidad del tratamiento de los mismo sin darte aviso, transfiriera tu datos a terceros sin el consentimiento del titular, obstruya los actos de verificación del Instituto o realice un uso ilegítimo de los datos.

IV. En caso de que persistan las infracciones de manera reiterada, el Instituto podrá imponer una multa adicional que irá de 100 a 320,000 días de salario mínimo vigente en el Distrito Federal. Tratándose de infracciones cometidas en el tratamiento de datos sensibles, los montos de las sanciones podrán incrementarse hasta por dos veces (IFAI, 2013).

Tomando en consideración las multas impuestas por el IFAI, es de suma importancia que las empresas desarrollen o implementen estrategias de seguridad que brinden protección a los datos personales de empleados, clientes entre otros datos que maneje la empresa.

El reglamento de la LFPDPPP explica de manera muy sencilla, los aspectos que una empresa u organización debe tomar en cuenta para no incurrir en una falta a la ley, la empresa debe tener a la mano dicho reglamento a la hora de implementar un estrategia de seguridad.

Capítulo III Modelos de arquitecturas de seguridad de la información ya existentes

3.1 Arquitecturas de seguridad de la información

Para poder desarrollar una propuesta de seguridad para una empresa privada, es necesario tener definido que es una arquitectura de seguridad, en qué consiste y cuantos tipos existen actualmente, de igual forma en el capítulo anterior se mencionaron los puntos importantes que debe tomar en cuenta una empresa privada para dar cumplimiento satisfactorio a la LFPDPPP.

3.1.1 Definición de arquitectura de seguridad de la información

Para poder tener una definición de arquitectura de seguridad de la información, vamos a retomar los conceptos que manejan algunos autores sobre el tema.

Lara (2012), define la arquitectura de un sistema, como un diseño estructural integrado; sus elementos y definiciones dependen de los requerimientos por lo que fue creada dicha arquitectura. Una estrategia de seguridad de la información debe apoyarse en un diseño que combine una infraestructura propia de seguridad y un esquema de servicios adecuado, que permita el cumplimiento en el manejo de la información.

Una estrategia de seguridad involucra un modelo a la medida que permitan cubrir con la mayor parte de las necesidades de seguridad que la organización requiere, en la cual se puede tener una infraestructura de seguridad de la información con una inversión propia y complementarla con un servicio de protección de datos y de monitoreo que correlacione todos los eventos de seguridad.

Rodríguez (2008), define la arquitectura de seguridad como el conjunto de controles de infraestructura de tecnologías de información recomendados para brindar, un ambiente que minimice los riesgos asociados a la utilización de tecnologías de información y apoye las estrategias de negocio.

Parada, et. al. (2010), dicen que la arquitectura es un esquema de acción estratégica en la organización, mediante el cual se establecen las directrices a nivel de seguridad de la información en cada uno de los procesos del negocio.

De igual forma en su escrito manifiestan que el Gobierno de Seguridad de la Información (GSI) define que para implementar un esquema de Seguridad de la Información, se debe tener en cuenta seis elementos, que necesariamente representan las intenciones de la Alta Gerencia en la formalización de un programa referente al tema de seguridad de la información.

1.- Alineación Estratégica: objetivos de seguridad alineados con los objetivos del negocio.

2.- Administración del Riesgo: dinamizar la forma en cómo se realiza y se da continuidad al análisis y tratamiento del riesgo, de tal manera que se reduzcan los riesgos y el impacto inherente a su materialización.

3.- Entrega de Valor: busca que la inversión realizada en seguridad de la información sea óptima, es decir, que sea proporcionado el valor del negocio y esta tenga un retorno de inversión.

4.- Administración de Recursos: administración efectiva y eficaz de los recursos asignados para la formalización de controles, políticas, roles y responsabilidades además de los presupuestos para seguridad de la información.

5.- Medición del Desempeño: definir indicadores que permitan medir los cambios de estado del negocio antes y después de la implementación de la seguridad de la información, como soporte y apoyo en los procesos del negocio.

6.- Integración: propósito o intención por hacer que los elementos mencionados en los ítems anteriores, converjan en un esfuerzo por asegurar el negocio, es decir, que sus procesos tengan un desempeño transparente antes, durante y después de su ejecución.

Tomando en cuenta los anteriores conceptos se puede decir que la arquitectura de seguridad de la información, es un conjunto de controles estructurados e integrados de tecnologías de la información, diseñados para brindar un ambiente más seguro y que minimice los riesgos de ataque, robo o mal uso de la información con la que cuenta una empresa u organización, sin afectar las actividades y apoyando las estrategias de dicha empresa.

3.2 Tipos de arquitecturas de seguridad de la información

Existen diferentes tipos de Arquitecturas de seguridad de la información, los cuales serán mencionados y explicados a continuación.

3.2.1 Arquitectura Empresarial (EA)

En el año de 1987 comienza la Arquitectura Empresarial, que tiene su inicio con la publicación en el diario de sistemas de IBM un artículo titulado "Un marco para la Arquitectura de Sistemas de Información ", por Jhon A. Zachman. En ese documento, estableció tanto el reto y la visión de las arquitecturas empresariales que guiarán el campo empresarial para los próximos años. El reto consistía en gestionar la complejidad de los sistemas cada vez más distribuidos.

Zachman (1987), dijo “El costo y el éxito de la organización reside en función cada vez más en sus sistemas de información que requieren un enfoque disciplinado para la gestión de esos sistemas.” La visión de Zachman sobre la agilidad y valor que las tecnologías de información podrían aportar al negocio se puede desarrollar de forma más afectiva a través del concepto de un arquitectura holística de sistemas, el lo describe como una arquitectura de sistemas de información. La arquitectura empresarial nace como disciplina que evoluciona desde modelos administrativos y de gestión, como la teoría organizacional y la teoría de sistemas.

La administración de las grandes organizaciones en relación a su sistema de información, es difícil; ya que dicho sistema cuenta con un conjunto de procesos que operan sobre una gran colección de datos estructurados que dependen en gran medida a las necesidades de la organización. Se recopila, elabora y distribuye la información, necesaria para las operaciones diarias de la organización y que son necesarias para las actividades de dirección, control y toma de decisiones en la organización.

Es por ello que la arquitectura empresarial tiene como principal objetivo mejorar la eficacia o eficiencia de la propia organización. Mediante innovaciones en la estructura de la organización, la centralización o la diversificación de los procesos de negocio, la calidad, la oportunidad comercial y la mejora continua en los proceso de Tecnologías de la Información.

La arquitectura empresarial en una organización corresponde a la forma de representar de manera integral la empresa, permitiendo cubrir y considerar todos y cada uno de los elementos que la conforman, esto conduce a una visión clara de los objetivos, metas y línea de negocios en la empresa, comenzando desde la perspectiva estratégica, hasta llegar a una descripción integrada, detallada y metodológicamente de la estructura actual y futura para los procesos de la organización; la cual incorpora algunos de los componentes que se consideran como críticos para su funcionamiento.

Entre los beneficios que obtiene una organización al implementar el modelo de arquitectura empresarial:

- Permite la identificación del estado actual de la empresa y la describe como una estructura coherente y articulada en todos sus componentes.
- Actúa como una fuerza integradora entre aspectos de planificación del negocio, de operación de la empresa y aspectos tecnológicos.
- Permite capturar la visión completa del sistema empresarial en todas sus dimensiones y complejidad
- Permite conocer de forma real, medible y detallada, la brecha que existe entre el estado actual de los procesos delos negocios y la tecnología que los soporta, respecto al estado requerido o deseado que exige la dirección estratégica.

3.2.2 Arquitectura de la seguridad

La arquitectura de seguridad según Killmeyer, (2001) quien lo describe con cinco elementos que serán explicados a continuación.

1.- Organización de la Seguridad e Infraestructura: es el reconocimiento de la necesidad de alinear procesos de negocio con la seguridad de la información, además declara la existencia de una persona encargada de su ejecución y gestión; dicha persona debe ser parte asesora o miembro de la Alta Gerencia en la organización, con el fin de conocer sus expectativas, logrando la alineación de la Alta Gerencia con la del Área de seguridad de la información.

2.- Políticas, Estándares y Procedimientos: elemento conformado por tres conceptos diferentes interrelacionados, el primero de ellos la política: es definida en términos de los objetivos del negocio y marcan la pauta para el comportamiento de los usuarios; los estándares son las buenas prácticas en sistemas de información; y los procedimientos definen el paso a paso, la forma como se desarrollan las diversas actividades por las personas encargadas de su ejecución.

3.- Líneas base de seguridad y la valoración del riesgo: debido a la gran demanda de esfuerzo en tiempo y dinero en pruebas de vulnerabilidad en los dispositivos. Killmeyer recomienda la definición de tres elementos que permiten manejar estas variables; las líneas base como una pauta para la configuración de dispositivos, a educación a los administradores y usuarios en el uso de las políticas de seguridad y evaluación de los controles, todo ello en un ciclo de realimentación continua.

4.- Capacitación y entrenamiento de los usuarios: es el proceso de concientización de los usuarios por parte de los encargados de la gestión en seguridad de la información para el negocio y enseñar la forma como se logran las mismas, al igual que las consecuencias de no atacarlas.

5.- Cumplimiento: este elemento es descrito como la etapa final del modelo, en cuanto es el mecanismo de revisión presupuesto para observar que lo definido en cada elemento corresponda realmente a las intenciones de la Alta Gerencia.

Cano (2004), manifestaba que la arquitectura de seguridad está sustentada en tres elementos que son los siguientes:

1.- Estructuras: reconocimiento de los procesos fundamentales que precisan la esencia que componen la seguridad de la información, entre estos se encuentran;

a) La información: reconocida como un activo.
b) Las estrategias del negocio: procesos que generan valor en su organización.
c) Los fundamentos de la seguridad informática: basados en los principios de confidencialidad, integridad, y disponibilidad como características de la información.
d) La administración de riesgos: que es la implementación de alguna metodología para descubrir vulnerabilidades y las estrategias para tratarlas y mitigar las amenazas.

2.- Procesos: llevar a cabo la implementación de las buenas prácticas de seguridad; propuesta basada en la norma internacional ISO 27002.

3.- Acuerdos: define la relevancia de establecer el canal de comunicación entre el área de seguridad de la información y la alta gerencia. Entre los aspectos a tener en cuenta se encuentran:

a) Establecimiento de prioridades de la alta gerencia.
b) Competencias y habilidades requeridas en el área de seguridad de la información.
c) Establecimiento y materialización del nivel de compromiso de la alta gerencia en los proyectos definidos en el área de seguridad de la información.
d) La definición y operación de los acuerdos de nivel de servicio.
e) Se propone compartir y alinear la agenda interna de la alta gerencia, con la de seguridad de la información.

3.2.3 Arquitectura de la Seguridad de la Información (ISA)

La arquitectura de seguridad de la información (ISA) se define como el ámbito de la protección de datos, de carácter personal, así como la implementación de códigos de buenas prácticas o recomendaciones sobre gestión de la seguridad de la información y de certificaciones internacionales, éstas últimas, relacionadas con la auditoría de los sistemas de información (Killmeyer, 2001).

El propósito principal de la ISA es asegurar que la misión de los procesos de negocio impulsados por los requisitos de seguridad de la información sea consistente, rentable y que los sistemas operen en equilibrio con la gestión de riesgos de la organización.

Tiene como objetivos:

- Apoyar, permitir y ampliar las políticas de seguridad, proporcionando seguridad orientada a la toma de decisiones. El resultado será estratégicamente alineado y coherente en toda la organización
- Proporciona seguridad relacionada con la aplicación de TI, así como los lineamientos en el diseño de la tecnología, sistemas y aplicaciones
- Reforzamiento de los eslabones más débiles de la organización y promover la coherencia
- Aplicabilidad en todo lo relacionado a la legislación y los requisitos reglamentarios existentes

Para resumir, la ISA proporciona una guía detallada que permite el seguimiento de los objetivos de mayor nivel y objetivos estratégicos de las organizaciones, a través de las necesidades específicas de protección de la misión, negocio, soluciones específicas de seguridad de la información proporcionada por las personas, procesos y tecnologías.

El Consejo Nacional de Investigación, Gobierno de EE.UU. (2002), “La Seguridad de la Información es la protección de la información y sistemas de información del acceso, uso, divulgación, alteración, modificación o destrucción con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información utilizada en una organización”. Dependiendo del entorno de la organización, se pueden tener diferentes amenazas que comprometan a los objetivos previamente mencionados.

3.2.4 Arquitectura de Seguridad de la Información Empresarial (EISA)

La Arquitectura de Seguridad de la Información se encarga de instituir una solución de seguridad de la información integral en la organización, que permita apoyar la seguridad en cada punto de la arquitectura, para que caminen al par de las metas comunes a la dirección estratégica.

Gartner (2006), menciona que el término EISA trata de reunir tres componentes indispensables que son: los dueños de la empresa u organización, los especialistas de la información y los implementadores de la tecnología como la ilustra la Figura 2.

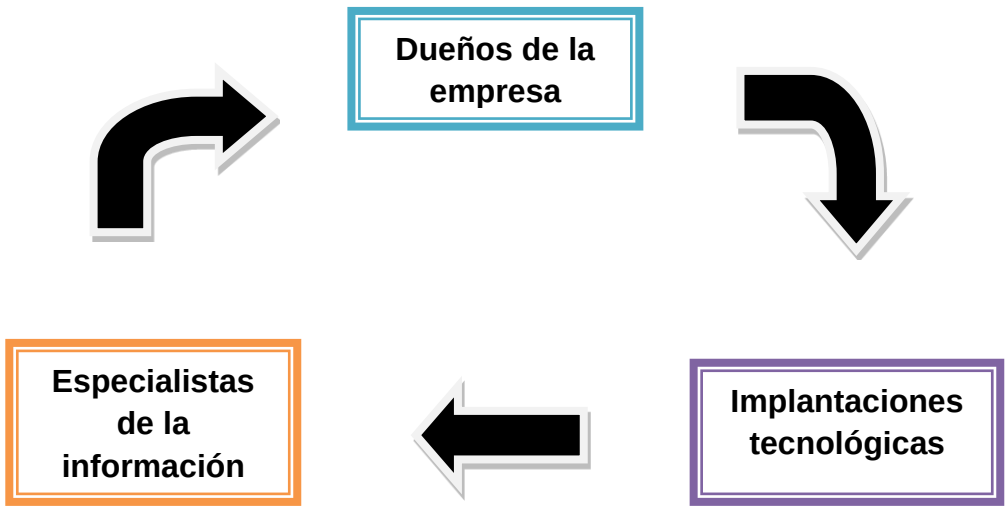

Figura 2 Elementos de la arquitectura de seguridad de la información empresarial (Creación propia).

Y dice ¨Si usted puede tener estos tres grupos juntos y unirlos detrás de una visión común que impulse el valor del negocio, usted ha tenido éxito, si no, ha fracasado. El éxito se mide en términos prácticos, como manejar la rentabilidad, no por la comprobación de los elementos de una matriz de proceso...¨

De igual forma es considerada como una herramienta que une la misión de la empresa y la estrategia de tecnologías de la información de una organización, vinculando la estrategia de inversiones en tecnologías de información y permitiendo asegurar una estrecha integración entre el negocio, las aplicaciones, la información, y las capas de la arquitectura de infraestructura, así como, involucra el desarrollo de una visión arquitectónica y la proyección del negocio hacia una meta u objetivo.

Una vez que esta visión se entiende bien, un conjunto de pasos intermedios se crean para ejemplificar el proceso de cambio en relación a la situación actual.

La EISA define un esquema de acción estratégico en la organización, mediante el cual se establecen las directrices a nivel de seguridad de la información que se proyecta implementar en cada uno de los procesos de negocio. Y tiene como objetivo poder garantizar la integridad, confidencialidad, disponibilidad y privacidad de la información que se maneja y procesa en la organización, así como una operación con un nivel de riesgo aceptable derivada del uso de las tecnologías de información asegurando la tranquilidad de directivos, funcionarios, clientes y socios de negocio.

Para cumplir con el objetivo se prevé el uso e implementación de métricas que permitan obtener un panorama general relacionado con el cumplimiento de los siguientes propósitos:

- Permitir la evaluación de la seguridad y el riesgo en la organización.
- Evaluar la situación actual de la seguridad de la información empresarial.
- Evaluación de los activos de información.
- Evaluación de los riesgos asociados con la implementación de nuevas tecnologías.
- Permitir la alineación del negocio hacia la seguridad

- Proporcionar una estructura, coherencia y cohesión con los procesos de negocio
- Asegurar que todos los modelos e implementaciones puedan ser diseñados hacia la estrategia de seguridad
- Establecer un lenguaje común para la seguridad de la información dentro de la organización
- Establecer procesos de mejora continua
- Establecer métricas de desempeño por cada área.

La arquitectura de seguridad de la información se ajuste a los cambios tecnológicas y permite responder a las nuevas amenazas y peligros. A manera de identificar los elementos y componentes requeridos para definir, diseñar, implantar, monitorear y auditar los requerimientos necesarios de seguridad.

La práctica de dicha arquitectura conlleva al uso de modelos conceptuales que detallan las organizaciones, los roles, las entidades y las relaciones que existen o deberían existir para llevar a cabo los procesos de negocio.

El producto final es una serie de modelos que describen en varios grados de detalle la operación actual del negocio y la identificación de los controles de seguridad que serán requeridos.

Dichos modelos, sirven de base para la toman de decisiones informadas sobre dónde invertir recursos, hacia dónde reorientar las metas organizacionales, los procesos, y las políticas en función del negocio.

Para implementar la EISA*,* generalmente se inicia documentando la estrategia de la organización. El proceso continua con la documentación de los procesos internos de negocio, y la forma en que la organización interactúa consigo misma y con sus clientes, proveedores, y otras entidades gubernamentales.

Habiendo documentado la estrategia y estructura de la organización, el proceso de la arquitectura se enfoca en los componentes tecnológicos tales como:

- Cuadros de organización, actividades, y flujo de procesos sobre cómo la *TI* de la organización opera
- Ciclos, periodos y distribución en el tiempo de la organización

- Proveedores de tecnología hardware, software y servicios
- Inventarios y diagramas de aplicaciones y software
- Interfaces entre aplicaciones (eventos, mensajes y flujo de datos)
- Intranet, Extranet, Internet, *e-commerce* (Comercio Electrónico)
- Clasificación de datos, bases de datos y modelos de datos soportados
- Hardware, plataformas, *hosting* (hospedaje web), servidores, componentes de red y dispositivos de seguridad
- Diagramación de los Niveles o Capas de seguridad de la organización
- Monitoreo y control de Accesos
- Redes de área local y abiertas, diagramas de conectividad a internet
- Sistemas de gestión para el tratamiento de la información interna.

La EISA, documentará el estado actual de los componentes técnicos de seguridad listados arriba, así como un estado ideal futuro deseado y finalmente un estado meta futuro resultado de los sacrificios y compromisos de ingeniería frente al ideal. Esencialmente el resultado es un conjunto de modelos anidados e interrelacionados.

Las dependencias de las tecnologías de información se han apoyado con el concepto *Information Technology Infrastructure Library* (ITIL) es un conjunto de libros en los cuales se encuentran documentados todos los procesos referentes a la provisión de servicios de tecnología de información hacia las organizaciones y contienen una serie de procesos para las mejores prácticas en el manejo de la información y mejora continua de los mismos.

Junto con los modelos y diagramas se debe implementar un conjunto de mejores prácticas dirigidas a la adaptabilidad de la seguridad, escalabilidad y manejabilidad de los procesos. Estas mejores prácticas de sistemas de ingeniería no son únicas a la EISA, pero son esenciales para su éxito.

La aplicación exitosa de la EISA, requiere una integración adecuada en la organización, ya que al tener todos los componentes técnicos documentados estos servirán de base para el crecimiento hacia las nuevas tecnologías requeridas por la organización a implementar.

La organización debe diseñar e implementar un proceso que asegure el movimiento continuo desde el estado actual al estado futuro. Para poder llegar a un estado futuro será mediante la realización de uno o los dos procesos siguientes:

- Disminución de la distancia presente entre la estrategia actual de la organización y apoyar la capacidad para dimensionar la evolución sobre seguridad en TI.

- Mejoras y sustituciones necesarias que deben hacerse sobre la arquitectura de seguridad de TI basadas en la factibilidad de proveedores del hardware y software, los requerimientos regulatorios conocidos o anticipados, y otros aspectos para la gestión funcional de la organización.

La EISA prevé convertirse en una práctica habitual dentro de las organizaciones, ya que las políticas de seguridad que se implementan son las líneas maestras de dicho contexto empresarial. La arquitectura que se obtiene es una combinación funcional de los procesos y la tecnología para alcanzar la meta de negocio. La EISA permite lograr la seguridad, y prestar asistencia jurídica y cumplimiento normativo.

El propósito fundamental de implantar una EISA, es para asegurar que la estrategia de negocio y la seguridad de las tecnologías de la información están alineadas. Como tal, la EISA permite la trazabilidad desde la estrategia de negocio actual hasta la tecnología subyacente.

Los beneficios que se esperan con la implementación de una EISA, es la de liderar e integrar de manera efectiva todos los asuntos relacionados con la arquitectura de negocio y de arquitectura tecnológica de TI en un ambiente institucional.

Los beneficios a la organización son:

- Lograr los objetivos estratégicos que dependen de recursos y capacidades de negocio asociadas con TI.

- Mejorar el desempeño del negocio al maximizar la eficiencia de TI a través de la organización.
- Incrementar la agilidad de la organización para identificar oportunidades y problemas potenciales, tomar decisiones y reaccionar rápidamente ante cambios.
- Establecer correctamente las prioridades de programas y proyectos, en cuanto a los requerimientos que rigen las soluciones basadas en TI.
- Vincular múltiples componentes asociados con TI, como lo son aplicaciones, sistemas, bases de datos y redes a través de la organización.
- Compartir eficientemente información entre líneas o unidades de negocio, así como con otras organizaciones.
- Integrar diversas aplicaciones y redes que carecían de estándares abiertos.
- Reducir los recursos duplicados de TI a través de la organización.
- Proteger integralmente los datos y activos críticos de información y de TI de acuerdo al nivel mínimo de riesgo aceptable para la organización.
- Asegurando inversiones de valor en TI.
- Mejorar la gestión del capital humano en áreas que requieren conocimiento y habilidades en TI, áreas tanto usuarias, como técnicas y operativas.

3.2.5 Modelo de Arquitectura de Seguridad de laInformación (MASI)

Es una propuesta estratégica para la administración de la seguridad de la información con base en los modelos anteriormente comentados. Según Parada et. al. (2008), afirman que la arquitectura MASI es un estrategia lógica conformada por cinco elementos: (1) negocio, (2) normativa, (3) gestión de la Arquitectura de seguridad de la información, (4) acuerdos e (5) infraestructura de seguridad de la información, y que cada uno de estos elementos es un proceso desarrollado mediante la asignación de actividades y tareas en seguridad de la información, pensadas y alineadas con los objetivos del negocio, ver Figura 3.

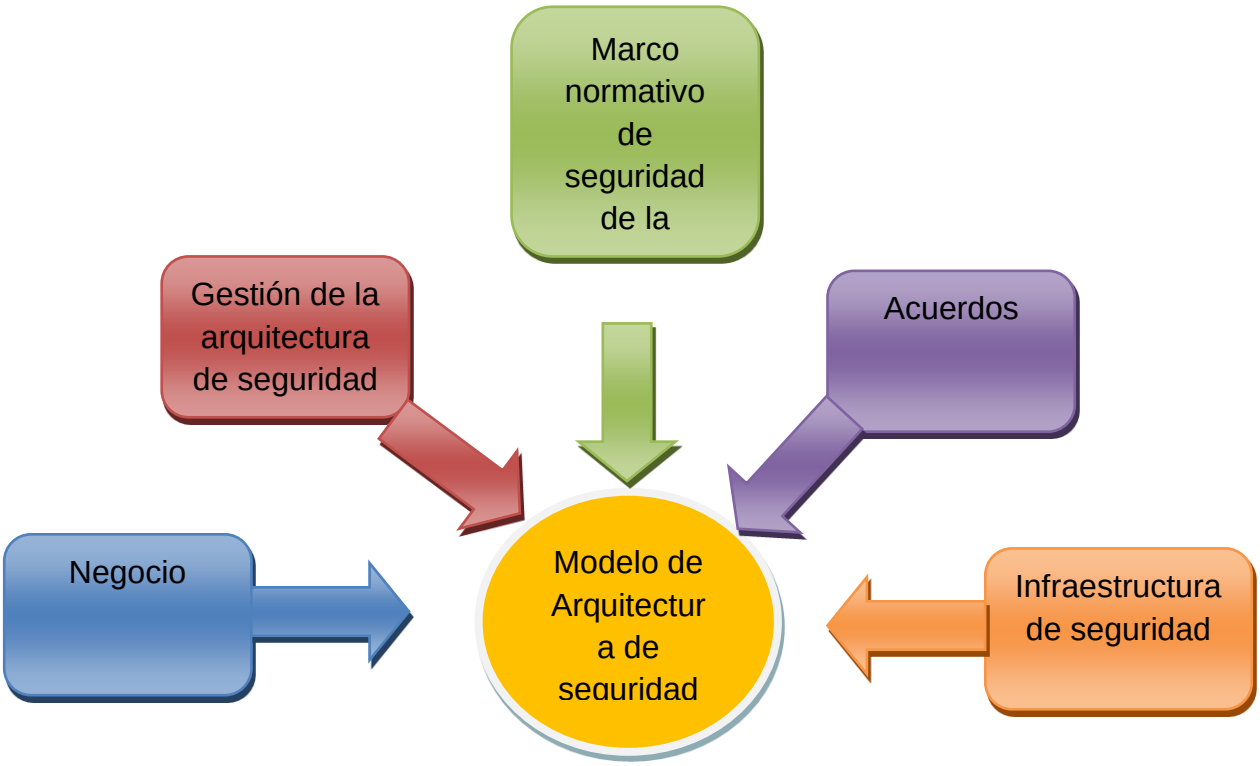

Figura 3. Elementos del modelo de arquitectura de seguridad informática (MASI) (Parada et. al., 2008)

A continuación explico el ciclo de vida del Modelo de Arquitectura de Seguridad de la Información (MASI) donde se desarrollan los cinco elementos del modelo:

Negocio

El objetivo de este elemento radica en la definición de estrategias de seguridad de la información, alineados con los objetivos organizacionales mediante el conocimiento detallado del negocio, para lograrlo se debe realizar un estudio y análisis de la siguiente documentación: la misión, la visión, el plan estratégico, las metas organizacionales, el cuadro de mando integral.

Análisis de riesgo

Mediante el análisis de riesgo se obtiene el conocimiento referente a:

- Las amenazas y vulnerabilidades que atentan contra los activos de información.
- Los controles existente para la mitigación de los riesgos.
- Probabilidad e impacto de la materialización de los riesgos.

Se debe tener en cuenta que el análisis de riesgo proporciona información referente a las necesidades de inversión de las organizaciones o empresas, enfocando a las necesidades en la mitigación de los riesgos existentes a través de la definición de los planes de tratamiento.

Motorización

La motorización permite la evaluación de los componentes de la arquitectura de seguridad de la información, el fin es determinar si la ejecución de los mismos está apoyando o no las estrategias del negocio, para ello se basa en tres tipos de monitorización que son los siguientes:

- **Monitorización técnica:** está enfocada en la ejecución de procedimientos de gestión de vulnerabilidad.

- **Monitorización de personal:** se identifica el nivel de sensibilidad de las personas involucradas (empleados, trabajadores y proveedores) respecto a seguridad de la información.

- **Monitorización operacional:** hace referencia a la monitorización de procesos; se requiere de la definición de un procedimiento de gestión de incidentes que permita la identificación de las faltas y la documentación de las soluciones, de tal forma que esto permita la mejora continua y el aprendizaje, procesos que realmente la arquitectura de seguridad de la información.

Actualización

Consiste en el proceso de mejoramiento de los elementos de la arquitectura de los elementos de la arquitectura, teniendo en cuenta los resultados de la monitorización y las posibilidades auditoras que se realicen al MASI.

Mantenimiento

El proceso de mantenimiento consiste en la implementación de las mejoras identificadas en la atapa de monitorización.

Entrenamiento

Como resultado del análisis de riesgo, de la monitorización y de las auditoras, surgen diferentes vulnerabilidades que deben ser tratadas a través de la realización de campañas que estén enfocadas en cambios a nivel cultural. Para ello se puede tener en cuenta la realización de: propaganda, cursos de capacitación. entre otras actividades.

El procedimiento para el desarrollo de la gestión de la arquitectura MASI es la siguiente:

1. Definir la metodología de gestión de riesgos.
2. Realizar una reunión con la Alta Gerencia para la aprobación de la metodología.
3. Aplicar la metodología de gestión de riesgos.

4. Definir los procedimientos de gestión de incidentes y gestión de vulnerabilidades técnicas.
5. Definir las actividades a desarrollar para la actualización de la documentación de la arquitectura.
6. Realizar la priorización de la implementación de las oportunidades de mejora identificadas.
7. Definir el proceso de gestión de la cultura de seguridad de la información.

MASI unifica dos modelos de infraestructura tecnológica de seguridad de la información los cuales son los siguientes:

- Modelos SAFE de Cisco, que define que la infraestructura de seguridad debe contemplar seis elementos que son: (1) identificación, (2) aseguramiento, (3) segregación, (4) resistencia, (5) correlación y (6) monitoreo; los cuales debe están enfocados en garantizar tanto la visibilidad como en control de la infraestructura (Mora, 2005).

- Modelo de Defensa en Profundidad de Microsoft, el cual dice que la infraestructura de defensa en profundidad debe garantizar seguridad a nivel de: datos, aplicación, equipos de cómputo, red interna y de perímetro (Cisco, 2009).

Con la unificación de los modelos establece los elementos de control definidos por el modelo SAFE de Cisco para garantizar la visibilidad, y el control debe ser definidos en cada uno de los niveles que define el modelo de defensa en profundidad de Microsoft.

Para la implementación es necesario desarrollar el elemento de infraestructura Tecnológica de seguridad y se deben llevar a cabo los siguientes pasos:

1. Identificar la plataforma tecnológica actual.

2. Identificar los elementos de seguridad informática disponibles en la red.

3. Evaluar las características de los elementos de seguridad frente los requerimientos de seguridad necesarios para establecer mecanismos de defensa en profundidad.

4. Una vez realizado el análisis se procede a identificar las oportunidades de mejora.

5. Realizar el diagrama de la infraestructura propuesta.

Ya teniendo definido la tecnología de seguridad con la cuenta, la empresa debe pasar a desarrollar el siguiente elemento que es el marco normativo de seguridad de la información, donde se tomaran en cuenta los puntos de seguridad que la empresa necesita como puede ser:

- Proteger información de actividades empresariales actuales o futuras.
- Proteger la información ante posibles fallas humanas.
- Prevenir la entrada de usuarios intrusos a información de la empresa.
- Vigilar el buen uso de la información.
- Cumplir con leyes de protección de información o datos personales.

Según Cano (2004), para desarrollar el elemento de los acuerdos es necesario establecer el medio o el canal de comunicación que garantice la integración del área de seguridad (proceso de seguridad) y la Alta Gerencia (expectativas del negocio), a fin de alinear los esfuerzos operacionales, tácticos y estratégicos del negocio.

Procedimiento para el desarrollo del elemento de acuerdos:

- Definir el canal de comunicación entre los encargados de la seguridad de la información y la Alta Gerencia.

- Realizar actividades de seguimiento continuo de las actividades desarrolladas por el área de seguridad a fin de identificar oportunidades de mejora.
- Definir un procedimiento de revisión continuo entre la Alta Gerencia y los encargados de la seguridad de la información.

Los beneficios de implementar este modelo de arquitectura de seguridad de la información son los siguientes:

- Se adapta a las necesidades de cualquier negocio, empresa u organización que desee implementarlo.
- Mejora el desempeño de la empresa en cuanto seguridad.
- Existe una mayor comunicación entre la organización.
- Se mantiene vigilada el área de tecnologías de información.
- Permite establecer un vínculo de comunicación entre seguridad de la información y la alta gerencia, de esta manera ambos saben la situación real de la empresa.
- Maximiza la eficacia y eficiencia de las tecnologías de información y comunicación.
- Se puede identificar rápidamente una falla o problema en las tecnologías de la información y darle solución de inmediato.
- Se tiene mayor control de la información con la que cuanta el negocio.
- Se cumple satisfactoriamente con leyes o normas de protección de *9información y datos personales.
- Reduce fallas en las tecnologías de información y comunicaciones.
- Vincula y vigila múltiples componente asociados con tecnologías de información como son: sistemas, bases de datos, hardware, redes, entre otros.

3.3 Estándares de seguridad existentes ISO

La Organización Internacional para la Estandarización, ISO por sus siglas en inglés (*International Organization for Standardization*), es una federación mundial que agrupa a representantes de cada uno de los organismos nacionales de estandarización que facilitan el comercio internacional (Solay, 2011).

Los estándares de seguridad de la información ISO fueron aprobados y publicados como estándares internacionales, en ellos se especifica los requisitos necesarios para establecer, implementar, mantener y mejorar un sistema de gestión de la seguridad, según el "Ciclo de Deming", PDCA acrónimo de *Plan, Do, Check, Act* que significa planificar, hacer, verificar, actuar.

Solay (2011), explica que la serie 27000 de seguridad de la información se compone de varios estándares que se explican a continuación:

- ISO 27000: Fue publicada en mayo de 2009. Contiene la descripción general y vocabulario a ser empleado en toda la serie 27000. Se puede utilizar para tener un entendimiento más claro de la serie y la relación entre los diferentes documentos que la conforman.

- UNE-ISO/IEC 27001:2007 “Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos”. Fecha de la de la versión española 29 noviembre de 2007. Es la norma principal de requisitos de un Sistema de Gestión de Seguridad de la Información. Los SGSI deberán ser certificados por auditores externos a las organizaciones, contempla una lista con los objetivos de control y controles que desarrolla la ISO 27002 (anteriormente denominada ISO17799).

- ISO 27002: (anteriormente denominada ISO17799).Guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información con 11 dominios, 39 objetivos de control y 133 controles.

- ISO 27003: En fase de desarrollo; probable publicación en 2009. Contendrá una guía de implementación de SGSI e información acerca del uso del modelo PDCA y de los requisitos de sus diferentes fases. Tiene su origen en el anexo B de la norma BS 7799-2 y en la serie de documentos publicados por BSI a lo largo de los años con recomendaciones y guías de implantación.

- ISO 27004: Publicada en diciembre de 2009. Especifica las métricas y las técnicas de medida aplicables para determinar la eficiencia y eficacia de la implantación de un SGSI y de los controles relacionados.

- ISO 27005: Publicada en junio de 2008. Consiste en una guía para la gestión del riesgo de la seguridad de la información y sirve, por tanto, de apoyo a la ISO 27001 y a la implantación de un SGSI. Incluye partes de la ISO 13335.

- ISO 27006: Publicada en febrero de 2007. Especifica los requisitos para acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información.

De acuerdo a lo anterior existen varias normas y arquitecturas que vigilan la seguridad de la información en las empresas, las cuales pueden ser implementadas brindar un grado de seguridad mayor a la información.

Capítulo IV Diseño de Arquitectura de Seguridad de Datos Personales para Empresas Privadas (ASDPEP)

4.1 Diseño de Arquitectura de Seguridad de Datos Personales para Empresas Privadas

En el siguiente capítulo se diseña una arquitectura de seguridad de la información, que se adapte a las necesidades de cualquier empresa privada, en la cual la finalidad fundamental es considerar la información personal con la que se trabaja y cumplir con la reglamentación de la ley federal de protección de datos personales en posesión de los particulares, sin afectar las actividades fundamentales de la empresa.

Para desarrollar esta nueva arquitectura, tomo en consideración algunos aspectos de las arquitecturas y normas que fueron mencionadas en el capítulo anterior como es:

- Arquitectura de Seguridad de la Información Empresarial (EISA).
- Modelo de Arquitectura de Seguridad de la Información (MASI).
- Norma ISO/IEC 27000.

4.1.1 Etapas de la Arquitectura de Seguridad de Datos Personales para Empresas Privadas (ASDPEP)

La Arquitectura de Seguridad de Datos Personales para Empresas Privadas (ASDPEP), consta de cinco etapas que se explican enseguida.

Primera Etapa: Análisis de la empresa

En esta etapa es necesario explicar cuál es la función de la empresa o negocio, cuáles son sus principales actividades, con qué información se trabaja y con que herramientas informáticas cuenta.

Se debe auxiliar de fichas de observación (Figura 4), aplicar entrevistas (Figura 5) a empleados y usuarios, analizar cuáles son sus tareas, con qué tipo de información se trabaja, cuales son los requerimientos de seguridad de la información, se deben detectar riesgos y vulnerabilidades. (Anexos 3 y 4)

ASDPEP

ARQUITECTURA DE SEGURIDAD DE DATOS PERSONALES PARA EMPRESAS PRIVADAS

FICHAS DE OBSERVACIÓN

NOMBRE DE LA EMPRESA:

_____

ÁREA OBSERVADA:_____

FECHA:_____ **HORA:**_____

ACTIVIDADES OBSERVADAS:

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

RIESGOS:_____
_____
_____
_____

VULNERABILIDADES:_____
_____
_____

Figura 4. Formato de fichas de observación

ASDPEP

ARQUITECTURA DE SEGURIDAD DE DATOS PERSONALES PARA EMPRESAS PRIVADAS

FICHAS DE ENTREVISTAS

NOMBRE DE LA EMPRESA:

_____

ÁREA ENTREVISTADA:_____

FECHA:_____ **HORA:**_____

1.- ¿Cuál es su principal función que realiza en esta área?

_____

_____

2.- ¿Trabaja con datos personales o con qué tipo de información?

_____

3.- ¿Cuenta con alguna contraseña para que ninguna persona ocupe su computadora?

Si ____ No_____

4.- ¿Cuántas personas ocupan esta máquina aparte de usted?

_____

5.- ¿Conoce la ley Federal de Protección de Datos Personales en Posesión de los Particulares?

_____

_____

4.- ¿Cuáles son las medidas de seguridad para la información?

_____

_____

_____

5.- ¿Cuentan con algún plan de contingencia, si se presenta alguna fallo o robo de información?

_____

_____

_____

6.- ¿Que tanto considera que conoce el sistema de información?

_____

_____

7.- ¿A quién recurre si se presenta algún problema o tiene alguna duda?

_____

_____

8.- ¿Considera que la información corre algún riesgo?

_____

_____

Figura 5. Formato de fichas de entrevistas

Segunda Etapa: Gestión de la Arquitectura (ASDPEP)

Esta etapa tiene como objetivo principal dar a conocer a la Alta Gerencia los requerimientos de tecnologías de seguridad, así como dejar en claro la información que desea proteger; los riesgos y la vulnerabilidad que se detectó en los sistemas de información de acuerdo con las observaciones y las entrevistas realizadas en la primera etapa.

De igual forma se pretende que el departamento de informática y la alta gerencia se encuentren en comunicación constante, para que sirva de base para la toma de decisiones oportunas. Deben de estar informados sobre dónde se debe de invertir más recursos, sobre las metas de la organización, procesos y política de la empresa.

Se le debe mostrar la documentación pertinente (Figura 6) a la alta gerencia, para la aceptación y aprobación de la implementación de la Arquitectura ASDPEP donde se deberá especificar los requerimientos detectados en la etapa anterior. (Anexos 5)

ASDPEP

ARQUITECTURA DE SEGURIDAD DE DATOS PERSONALES PARA EMPRESAS PRIVADAS

Formato de Aceptación de la Implementación de la ASDPEP

Nombre de la empresa_____

Lugar y Fecha_____

Nombre del encargado de la Alta Gerencia_____

Requerimientos detectados en la Etapa de Análisis de la empresas:_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Firma de aceptación de la Alta Gerencia

_____

Nombre y Firma

Figura 6. Formato de aceptación de la implementación de la ASDPEP

Tercera Etapa: Marco normativo en base a la LFPDPPP

En esta etapa se debe revisar las disposiciones generales de la LFPDPPP, así como nombrar a un representante del tratamiento de los datos personales recolectados y está obligado a vigilar por el cumplimiento de los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la ley.

La ley solicita a las empresas privadas trabajen en la elaboración, diseño y difusión de un aviso de privacidad, algunas recomendaciones generales para su diseño y presentación son las siguientes:

- Contar con títulos cortos, y claros, que de manera sencilla informen al titular sobre el contenido del aviso.
- Utilizar un lenguaje claro y comprensible acorde, a fin de que el mensaje se dirija de manera adecuada el público objetivo.
- Brindar un contexto para facilitar la comprensión del contenido.
- Tener una estructura clara y textos breves.
- Evitar la inclusión de textos o formatos que induzca al titular elegir entre una o varias opciones, negar o afirmar algo en específico.

A continuación se presenta un formato de cómo puede redactarse un aviso de privacidad. Ver Figura 7 (revisar el anexo 6)

AVISO DE PRIVACIDAD

[Nombre o razón o denominación social y comercial del responsable], con domicilio en [señalar calle, número, colonia, ciudad, municipio o delegación y entidad federativa], es responsable de recabar sus datos personales, del uso que se le dé a los mismos y de su protección.

Su información personal será utilizada para proveer los servicios y productos que ha solicitado, informarle sobre cambios en los mismos y evaluar la calidad del servicio que le brindamos. Para las finalidades antes mencionadas, requerimos obtener los siguientes datos personales: [dato 1], [dato 2], considerado como sensible según la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, [dato 3] y [dato 4].

Usted tiene derecho de acceder, rectificar y cancelar sus datos personales, así como de oponerse al tratamiento de los mismos o revocar el consentimiento que para tal fin nos haya otorgado, a través de los procedimientos que hemos implementado. Para conocer dichos procedimientos, los requisitos y plazos, se puede poner en contacto con nuestro departamento de datos personales en [*datos de contacto, domicilio, teléfono, coreo electrónico*] o visitar nuestra página de Internet [*dirección electrónica*].

Asimismo, le informamos que sus datos personales pueden ser transferidos y tratados dentro y fuera del país, por personas distintas a esta empresa. En ese sentido, su información puede ser compartida con [señalar el tipo de destinatarios de estas transferencias], para [describir finalidades]. Si usted no manifiesta su oposición para que sus datos personales sean transferidos, se entenderá que ha otorgado su consentimiento para ello.

□ No consiento que mis datos personales sean transferidos en los términos que señala el presente aviso de privacidad.

Si usted desea dejar de recibir mensajes promocionales de nuestra parte puede solicitarlo a través de [*teléfono, dirección, correo electrónico*].

Cualquier modificación a este aviso de privacidad podrá consultarla en [señalar medio].

Fecha última actualización [día/mes/año]

Figura 7. Formato de aviso de privacidad (IFAI.com)

Es importante tomar en cuenta que cualquier titular de los datos, o en su caso su representante legal, podrá ejercer los derechos de acceso, rectificación, cancelación y oposición previstos en la Ley. El ejercicio de cualquiera de ellos no es requisito previo ni impide el ejercicio de otro. Los datos personales deben ser resguardados de tal manera que permitan el ejercicio sin dilación de estos derechos; de igual forma el responsable de los datos debe dar atención inmediata a cualquier demanda de algunos de los derechos ARCO.

Cuando el responsable pretenda transferir los datos personales a terceros nacionales o extranjeros, distintos del encargado, deberá comunicar a los titulares en el aviso de privacidad y las finalidades a las que el titular sujetó su tratamiento. El tratamiento de los datos se hará conforme a lo convenido en el aviso de privacidad, el cual contendrá una cláusula en la que se indique lo que se pretende hacer con sus datos.

Cuarta Etapa: Diseño y desarrollo de la Arquitectura

En la cuarta etapa se debe planificar y diseñar la arquitectura de seguridad de los datos, es necesario comprender en su totalidad las actividades de la empresa, determinar cuáles son los datos personales con los que se trabajan. Se debe presentar un informe del diseño a la alta gerencia, que representa un estatuto escrito que define el problema, de acuerdo al análisis de hechos relevante de las etapas anteriores.

Esta etapa se basa en los resultados de las etapas anteriores, y comenzará el diseño de una nueva estrategia para proteger los datos, se puede auxiliar de herramientas de seguridad para información como las siguientes.

1. Si la empresa privada cuenta con una red interna que requiere ser protegida:

    a) Router o Enrutados, que es un sistema para la interconexión de redes informáticas que permite asegurar el enrutamiento o direccionamiento de paquetes entre las diferentes redes y también se encargan de resolver cual es la mejor ruta para él envió del paquete de datos**.**

Como herramienta de seguridad, algunos enrutadores proporcionan un complemento más a la seguridad, ya que permiten la asignación de direcciones NAT (*Network Address Translation* o Traducción de Dirección de Red), que resulta en transformar una dirección IP pública en varias direcciones IP privadas, de tal forma que resulta difícil para los intrusos detectar la dirección IP de alguna computadora detrás de un *router*,

b) *Firewall* o Cortafuego, es un sistema de defensa ubicado entre dos redes y que sirve como un filtro para permitir o bloquear el acceso a un servicio, dependiendo de reglas previamente establecidas. Consta de un dispositivo o conjunto de dispositivos de software o de hardware configurados para prevenir accesos no deseados a una red como primer punto de contención.

   El cortafuego funciona definiendo una serie de permisos para la comunicación, tanto de entrada como de salida, mediante reglas que se pueden hacer teniendo en cuenta los puertos de comunicación, los programas o las *IP* de conexión.

c) El Sistema de Detección de Intrusos IDS, es un sistema de seguridad que se encarga de identificar posibles violaciones de seguridad o mal uso de recursos, hace un análisis en tiempo real del tráfico en la red mediante el uso de librerías de registros o firmas.

Cuando encuentra una anomalía o uso no autorizado solo genera alertas. Generalmente se pone después de un *firewall*, para evitar falsos positivos o coincidencias que no representan una amenaza.

2. Para proteger la información privada que se encuentre en las computadoras:

    a) Colocar una contraseña de administrador, es la contraseña más común y sencilla que garantiza seguridad para la información de una computadora y puede crearse más de una cuenta si la maquina se requiere compartir con otra trabajador.
    b) Contraseña del BIOS, nadie podrá hacer uso de la computadora si no cuenta con la contraseña del BIOS ya que es el primer programa que la computadora ejecuta cuando se enciende de esta forma nadie podrá acceder a la computadora si no sabe la contraseña.
    c) Si por alguna razón ya entro al sistema operativo de la computadora y no es persona autorizada para tener acceso a la información privada, no podrá hacerlo, ya que el sistema que contiene toda la información personal cuanta con una contraseña que solo el personal autorizado posee, esta contraseña debe agregarse a la programación del sistema.

d) Se bebe crear una copia de seguridad de la información por algún desastre o fallo que no esté en nuestra posibilidad de detener.

Es muy importante evitar el acceso no autorizado tanto al sistema informático como al recinto o lugar donde se encuentre ubicado, es una parte muy importante dentro de la seguridad y para eso existen los sistemas de protección.

Todas estas medidas de protección formaran parte de la seguridad activa, ya que se utilizan para evitar el acceso de un usuario no autorizado que podría comprometer tanto la privacidad como la integridad de la información contenida en el sistema informático.

Algunos sistemas de control de acceso pueden ser: guardias y cámaras de seguridad que son utilizados para evitar el acceso al edificio tanto exterior como interior y así controlar el acceso a lugares restringidos. El uso de llaves para acceder al edificio o a la habitación donde se encuentran los equipos, así como llaves para bloquear el equipo en sí.

Para tener un control del personal que puede ingresar a los equipos se encuentra el acceso biométrico mediante huella dactilar, además de estos sistemas más usuales, existen otros más complejos y que están empezando a ser utilizados por grandes organizaciones, como los sistemas de identificación por radiofrecuencia, sistemas de token mediante envíos de mensajes desde el celular, entre otros.

Este análisis del diseño ha sugerido la implementación de un conjunto detallado de herramientas que ayudarán al sistema a estar protegido de intrusos y el equipo de informática ha decidido cuál es la mejor alternativa, que resolverá de mejor manera el problema o las necesidades de la empresa.

El informe de diseño debe contener los siguientes aspectos ver Figura 8:

- Las especificaciones de diseño de los procedimientos y operaciones que se van a modificar.
- Las herramientas de seguridad que se van a utilizar, las razones de la elección, y las opciones que se consideraron.
- Los efectos que quizá tengan estos cambios sobre la estructura de la empresa así como para las instalaciones de redes o de la ubicación de las maquinas.
- Los probables efectos sobre el personal de cuanto se dispone para llevar a cabo la arquitectura, si debe contratar a más personal o si se le debe de brindar una capacitación al personal ya existente.
- Un resumen de los problemas que podrán surgir y de las ventajas que representa el cambio.

ASDPEP

ARQUITECTURA DE SEGURIDAD DE DATOS PERSONALES PARA EMPRESAS PRIVADAS

Formato de informe de Diseño de la ASDPEP

Nombre de la empresa_____

Lugar y Fecha_____

Nombre del encargado de la Alta Gerencia_____

De acuerdo con las etapas de la Arquitectura es necesario implementar las siguientes herramientas:_____
_____

Para la implementación de las herramientas es necesario si/no contratar personal especializado como es:_____
_____

Se debe considerar los siguientes cambios en la estructura de la empresa:_____
_____

Se deberá capacitar al personal para que hagan uso adecuado de las herramientas para cumplir con los requerimientos de la LFPDPPP si /no porque:_____
_____
_____

as ventajas de la implementación de la arquitectura son las siguientes
_____
_____

Firma de aceptación de la Alta Gerencia

_____

Nombre y Firma

Figura 8. Formato de informe de diseño

Quinta Etapa: Implementación, pruebas, capacitación y evaluación

Una vez aceptado el diseño y especificado las herramientas que se requieren para el cumplimiento de la ley, es necesario continuar con la implementación, que es instalar o modificar la configuración de los equipos, redes o sistemas de información. Esto debe ser realizado por personal especializado en el tema, para evitar fallos más adelante.

En cuanto están implementadas las herramientas de seguridad y se modifico lo necesario se continúa con las pruebas para buscar algún error o posibles fallos, las pruebas se deben hacer de todas las formas posibles para disminuir el porcentaje de error.

Se debe capacitar al personal que va a utilizar los equipos y los sistemas, para que tenga noción de cómo trabajan, como funcionan, que hacer en caso de algún fallo o si detecta algún cambio, de igual forma es necesario que el personal que labora en la empresa firme un contrato de confidencialidad para que asiente mayor atención en la información que maneja y la convierta en confidencial.

Una vez comprometido y capacitado el personal se hacen pruebas y se evalúa cómo funcionan los cambios y que tan productiva es la implementación de la arquitectura ASDPEP.

Se debe entregar un reporte a la alta gerencia que contenga la siguiente información Figura 9 (Ver Anexo 8):

- Quienes realizaron la implementación de la Arquitectura.
- Especificar si se encontraron fallas a la hora de hacer las pruebas y mencionar de que tipo y como las resolvieron.
- Hacer un listado del personal que tomo las capacitaciones, el cual lleve la firma de conformidad de la capacitación que recibieron.
- La alta gerencia debe realizar una evaluación de la implementación de la arquitectura y se debe firmar de conformidad, tanto alta gerencia como el departamento de informática.

ASDPEP

ARQUITECTURA DE SEGURIDAD DE DATOS PERSONALES PARA EMPRESAS PRIVADAS

Formato de Informe implementación, pruebas, capacitación y evaluación de la ASDPEP

Nombre de la empresa_____

Lugar y Fecha_____

Nombre del encargado de la Alta Gerencia_____

Nombre de los responsables de la implementación de la ASDPEP:_____
_____
_____
_____
_____

Se detectaron fallas en las pruebas si/ no cuales:_____
_____
_____
_____
_____

Nombre y puesto de los empleados que recibieron la capacitación así como la firma de conformidad con la capacitación:_____
_____
_____
_____
_____
_____

Calificación que obtuvo la implementación de la Arquitectura ASDPEP según la evaluación de la alta gerencia:_____
_____

Firma de aceptación de la Alta Gerencia

_____

Nombre y Firma

Firma de aceptación Depto. de Informática

_____

Nombre y Firma

Figura 9. Formato de informe de la Implementación, pruebas, capacitación y evaluación

De esta forma se concluye la implementación de la Arquitectura de Seguridad de Datos Personales en Posesión de una Empresa Privada, cuya finalidad principal fue el cumplimiento satisfactorio a la LFPDPPP y de esta manera la empresa privada no tendrá que preocuparse por esta ley.

Conclusiones

Actualmente México cuenta con una legislación de protección de la información, como es ley federal de protección de datos personales en posesión de los particulares, que es la encargada de salvaguardar la integridad y vigilar que sean utilizados únicamente para el fin para el que fueron solicitados por a una o más empresas de carácter privado.

Sin embargo, en algunos casos las empresas privadas no cuentan con las herramientas informáticas necesarias para dar cumplimiento satisfactorio a la ley, en este sentido el trabajo que se entregó a dicha institución como propuesta de análisis, responde a sus necesidades y condiciones, tal y como se planteó inicialmente en el objetivo:

- Analizar la ley federal de protección de datos personales en posesión de los particulares, para garantizar la implementación y cumplimiento de la misma mediante consideraciones en la seguridad de la información.

Para cumplir con el objetivo, el documento de tesina incluye un análisis FODA para entender las razones para implementar la ley y las herramientas de seguridad de la información en México, de igual forma contienen una breve reseña de los factores que influyeron para la creación y aprobación de la ley.

El trabajo realizado permite que cualquier persona conozca más acerca de los principios fundamentales de la ley, las disposiciones generales que deben ser cumplidas, los derechos que otorga la ley a los propietarios de los datos y las obligaciones que deben cumplir las empresas privadas para no incurrir en algún delito.

Se investigó la función de la seguridad informática y de la seguridad de la información, así como los beneficios que presenta un sistema de información cuando es implementada una herramienta de seguridad, dichos beneficios pueden ser internos o externos al sistema de información donde son almacenados y tratados los datos personales. Se analizó la conexión que existe entre la ley y la seguridad de la información, recopilando información sobre vulnerabilidades y riesgos que se presentan con mayor frecuencia en los sistemas de información y que dan como resultado un uso inadecuado de los datos personales.

En el capítulo IV se diseñó una propuesta de arquitectura de seguridad de la información, en base a unas ya existentes, las cuales fueron analizadas y dieron como resultado una arquitectura llamada ASDPEP, Arquitectura de Seguridad de Datos Para Empresas Privadas, como se propuso en un principio en los objetivos específicos.

Una de las principales razones para la creación de la arquitectura es sin duda que las entidades privadas le están dando mayor importancia al manejo de la información con la que cuentan, estableciendo políticas, procedimientos y normas, para la protección de los datos.

La arquitectura es una herramienta que permite detectar fallas, vulnerabilidades o riesgos que sean una amenaza para la integridad de los datos personales con los que trabaja la empresa y que es su responsabilidad dar un uso adecuado, cumpliendo con la normatividad de la ley de protección de datos personales.

Por lo que la implementación de la arquitectura ASDPEP, puede cubrir necesidades de seguridad requeridas en las empresas privadas y ayudar al cumplimiento de la ley. Las empresas no se pueden permitir el privilegio de tener fugas no controladas, es por esto que la implementación de ASDPEP, les permitirá reforzar las medidas de seguridad con las que cuentan.

Un punto valioso de la arquitectura es que permite a cualquier empresa conocer los principales procesos que llevan a cabo diariamente, para elegir una tecnología de seguridad de la información que se adapte a las necesidades de su organización. Debe de empezar por identificar sus actividades y recursos principales con los que trabaja, revisar las políticas definidas en la ley, detectar los eventos potencialmente vulneradores que impidan la funcionalidad de cada área.

Con la arquitectura diseñada en el trabajo de tesina, las empresas privadas:

- Contarán con una solución que se adecua a sus necesidades de seguridad para la protección de los datos personales.
- El departamento de Seguridad Informática, contará con una herramienta que le permita descubrir, monitorear y proteger la información que fluye dentro y fuera de la red, ante cualquier uso indebido.
- Reforzará políticas de seguridad Interna.
- Administrará de manera sencilla la información durante todo su ciclo de vida.
- Regulará a los usuarios en el correcto uso de su información.
- Se encargará del cumplimiento satisfactorio de la ley de protección de datos.

Una de las bondades del presente trabajo es que la Arquitectura de Seguridad de Datos Personales para Empresas Privadas, puede ser retomada para otro proyecto de investigación como una tesis, en la cual se compruebe si es factible su implementación y si cumpla con las exigencias de la empresa y del cumplimiento de la Ley Federal de Protección de Datos Personales. Ya que en este trabajo de Tesina no se comprobó en un caso práctico la factibilidad de la arquitectura.

Bibliografía

- Aceitung, C. (2006). Seguridad de la información. México D.F. LIMUSA Noriega Editores. Pp. 30, 31, 32, 33, 34, 35.

- Agencia de Protección de datos (1999) XX Conferencia Institucional de autoridades de protección de datos 1999. Madrid, España. Editorial agencia de protección de datos. P.p. 55, 56, 56, 59, 60.

- Arenas, R. (2006) El derecho fundamental a la protección de datos personales en Europa. Valencia, España. Tirant lo Blanch. P.p. 71, 72, 73, 75, 76.

- Borghello C. (2001) Tesis de Seguridad Informática, sus aplicaciones e implementaciones. Buenos Aires. Universidad Tecnológica Nacional. P.p. 89, 90, 91.

- Cano, J. (2004) Inseguridad Informática: "Un concepto dual en Seguridad Informática".
  Disponible en Internet: http://www.acis.org.co/fileadmin/inseg-inf.pdf.

- Cisco, Cisco (2009) SAFE Solution Overview. Estados Unidos. Cisco.

- Civitas, T. (2006) Revista española de protección de datos. PUOLET Julio- Diciembre
  Disponible en Internet:
  http://ieaip.org.mx/biblioteca_virtual/datos_personales/siodf.

- Coello, A. (2003). Breve historia de la computación y sus pioneros. México, D.F. Fondo de Cultura Económica. Pp. 60,61, 62, 63.

- Collins, J. (2000) Computación Fácil. México. ALEC SA de CV. Pp. 70, 73, 74, 75, 76.

- Córdoba, G. (2005). La Investigación Tecnológica. México. Editorial LIMUSA. Pp. 81, 82, 143, 144, 145, 230, 231.

- Daltabut, E. (2007). La seguridad de la información. México. LIMUSA. Pp. 70, 71, 72, 73, 74.

- Diario Oficial de la Federación 2010. Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

- Donald H. (1995). Informática Presente y Futuro. México. Mc Graw Hill. Pp. 100, 112, 113.

- Escobar, B. (1997). La evolución Económica de los Sistemas de Información. Sevilla, España. Editorial de la Universidad de Sevilla. Pp. 100, 101, 102, 103, 104, 105.

- Espinoza, R. (2009). Seguridad Informática, estudio de percepción de seguridad de la información en México. Universidad Interamericana. Disponible en Internet: http//regulan.espacio.com/post/2010/03/04/seguridad-informatica-percepcion-seguridad-la

- Firman. S. (2005). Seguridad Informática, MP Ediciones. España. Pp. 87, 88, 89, 90.

- Gartner Consulting (2006), “Incorporating Security into the Enterprise Architecture Process.” Whitepaper Disponible en Internet: http://www.gartner.com/DisplayDocument?ref=g_search&id=488575.

- Gómez, A. (2007). Enciclopedia de la Seguridad Informática, 1era Edición. México. AlfaOmega Grupo Editorial S.A. de C.V. Pp. 70, 71, 72, 73.

- Gómez, C. (1994) Sistemas Administrativos. México. Mc Graw Hill. Pp. 100, 101, 102, 103.

- González, P. (2012). Biblioteca Jurídica Virtual del Instituto de Investigaciones jurídicas de la UNAM
  Disponible en Internet:
  http://biblio.juridica.unam.mx/revista/derechosinformacion/20/art/art1.pdf

- Gutiérrez Juan. Seguridad Digital y Hackers, Ediciones Anaya. Madrid, 2005.

- Hornos, M.; Abad, M. (1998). La gestión de la información como para adquirir ventaja competitiva: las MIS en alta gerencia. Barcelona, España, Editorial Mayo. Pp. 69, 70, 72, 73, 77.

- ifai.org.mx 08/02/2013 10:18

- Kidwell, P.; Ceruzzi, E. (1994). Londmarksin Digital Computing: A Smithsonian Pictorial History, Washington, DC, Smithsonian Press. Pp. 89, 90, 91, 92.

- Killmeyer T. (2001). Information Security Architecture “An Integrated Approach to Security in the Organization”, Auerbach, Washington, D.C.

- Lara, C. (2012). Tesina Análisis de tecnologías sobre seguridad para dependencias de gobierno (SSP). UEAM Texcoco. México, Pp. 55, 56, 57, 58, 60.

- American Psychological Association (2001). Publication Manual of the American Psychological Association. Washington, DC. Firth Edition. Pp. 387, 388, 389, 390, 392.

- Molina, R. (2005). Instalaciones y mantenimiento de redes locales. México. Editorial Alfaomega.

- Mora, C. (2005). Implementaciones de sistemas de información seguros". Honduras.

  Disponible en internet

  www.iimv.org/actividades2/05Tecnolog/Microsoft.ppf.

- Ortega, S. (2008). Actuaciones Inspectoras en Materia de Protección de Datos. España. J.M. Busch. Pp. 130, 131, 132, 133.

- Parada, J.; Calvo, A.; Flórez, A. (2010). Modelo de Arquitectura de Seguridad de la Información

  Disponible en Internet:

  http://www.iiis.org/CDs2010/CD2010CSC/CISCI_2010/PapersPdf/CA626FI.pdf

- Rayn, S. (2012) Manual de seguridad.

  Disponible en Internet:

  http://www.manualdeseguridad.com.mx/aprende_a_protegerte/seguridad_en_la_informacion/seguridad_en_la_informacion_opi.asp

- Rojas, S.; Sánchez, P. (2012). Leyes de Protección de Datos Personales en el Mundo y la Protección de Datos Biométricos parte I y II.

  Disponible en Internet:

  http://revista.seguridad.unam.mx/numero-13/leyes-deprotecci%C3%B3n-de-datos-personales-en-el-mundo-y-la-protecci%C3%B3n-de-datos-biom%C3%A9tricos-%E2%80%93

- Rodríguez, M. (2008) Diseño de Arquitectura de Seguridad.

  Disponible en Internet:

  http://oitel.univalle.edu.co/cit/actas/2008/Anexo_Acta_7_Diseno_de_Arquitectura_de_Seguridad.pdf

- Sanders, D. (1995). Informática Presente y Futuro. Washington, DC Mc Graw Hill., Pp. 50, 52, 53, 54.

- Solay, M. (2011). Seguridad de la Información y Seguridad Informática.

  Disponible en Internet:
  http://www.manualdeseguridad.com.mx/aprende_a_protegerte/seguridad_en_la_información.asp.

- Shurkin, N. (1996). Norton Engines of the Mind: The evolution of the computer from Maintramees to Michoprocessers. New York City, Pp. 70, 71, 78, 79.

- Téllez, V. (2009). Derecho Informático. México D.F. Mc Graw Hill. Pp. 30, 31, 33, 34.

- Troncoso, R. (2010). Comentarios a la Ley Órganica de Protección de Datos de Carácter Personal. Madrid, España. Civitas. Pp. 20, 21, 22, 23, 30, 31, 35, 50.

- Verdaguer, L. (2010). 1000 Soluciones de Protección de Datos. Madrid, España. Editorial CISS. Pp. 67, 68, 69, 70, 72, 75.

- Zachman, J. (1987) Framework for Information Systems Architecture, Boston, E.U. IBM Systems Jurnal. Pp. 80, 81, 82, 83.