UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

BUENAS PRÁCTICAS PARA PROTEGER DATOS CONFIDENCIALES EN LAS ASEGURADORAS

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

INGENIERA EN COMPUTACIÓN

P R E S E N T A :

MIRIAM JOSEFINA PADILLA ESPINOSA

DIRECTORA DE TESIS:

M.C. CINTIA QUEZADA REYES

MÉXICO 2009

AGRADECIMIENTOS

"El agradecimiento es la memoria del corazón."

Autor anónimo.

A mi madre Ana Guadalupe Espinosa Contreras:

Por ser la fuente de luz y motivación durante este camino, por tus consejos llenos de sabiduría, tu dedicación, tu fuerza. Por siempre brindarme apoyo incondicional pero sobre todo por tu amor.

Viviré eternamente agradecida por haberme dado la vida y hacer día a día de mí la mujer que soy.

Con todo mi amor por siempre te dedico a ti principalmente el fruto de mi trabajo que dará como resultado la culminación de una etapa académica, pero el inicio de mi vida profesional.

A mi padre Ramón Padilla Vázquez *por todo tu apoyo, por llenar mi vida del espíritu de lucha constante, por tu esfuerzo para lograr darme una carrera profesional, por siempre agradecida te estaré.*

A ti abuelita linda *que Dios decidió que en este momento tan importante estuvieras desde el cielo mirándome. Gracias por todo tu amor, tu dedicación, tu enseñanza, vives y vivirás por siempre en mi mente y en mi corazón.*

A todos mis tíos *que desde pequeña me han brindado todo su cariño.*

A mis tías Rosy y Vero *por todo su cariño y su apoyo que ha contribuido para el logro de esta meta tan importante en mi vida.*

A ti Osky *por iluminar mi vida con tu amor, tu apoyo por motivarme siempre a vencer mis miedos, por enseñarme que para el verdadero amor nunca hay obstáculos ya que: "Cuando dos personas se aman nada es imposible".*

A la M.C. Cintia Quezada Reyes *por todo su apoyo y tiempo dedicado para la culminación satisfactoria de mi tesis, por su hermosa amistad y por todas aquellas oportunidades que me ha brindado.*

Al Dr. Enrique Daltabuit *por su apoyo, sus asesorías y el tiempo dedicado a enriquecer con sus conocimientos el contenido de mi tesis.*

A mis entrañables amigos Mario, Jiri, Memo, Karlita, Fer, Kuthumi, Miguel Rodríguez, Emmi, Anaid y Paquito *porque aunque el tiempo pase siempre están cerca de mí para compartir mis tristezas y mis alegrías gracias por su amistad.*

A la Mtra. Artemisa Pedroza de De Gortari *porque durante mi estancia en la Coordinación a su cargo me permitió conocer a la persona maravillosa que es, gracias por todos sus consejos, su apoyo, su amistad y su cariño. La llevaré por siempre en mi corazón.*

A todos y cada uno de mis profesores de la Facultad de Ingeniería *por todos sus conocimientos impartidos que serán las herramientas para defenderme en la vida*

profesional, gracias a todos aquellos que me dieron la oportunidad de conocerlos más allá del ámbito académico y que me han brindado su amistad.

Es y será por siempre un honor ser egresada de la Universidad Nacional Autónoma de México. Gracias a mi alma mater por mis profesores, mis amigos, por todos y cada uno de los momentos maravillosos e inolvidables que he vivido en sus bellas instalaciones y que han contribuido a mi formación no sólo académica sino humana.

"POR MI RAZA HABLARÁ EL ESPIRITÚ"

_____

Miriam Josefina Padilla Espinosa

ÍNDICE

ÍNDICE

INTRODUCCIÓN

La creciente demanda por la difusión, obtención, procesamiento y almacenamiento de la información a través del uso de medios electrónicos ha dado como resultado que las organizaciones requieran la implementación de controles que brinden mayor protección hacia sus activos, ya sea mediante las políticas de seguridad, las buenas prácticas, los métodos de cifrado, los controles de acceso más sofisticados, entre otras alternativas, que les permitan garantizar la seguridad en la información que es utilizada para el desempeño de las actividades del negocio y de esta forma garantizar que se cuenta con la confidencialidad, la integridad y la disponibilidad de la información a su cargo.

Este es el punto de partida sobre el cual se sustenta este trabajo que está enfocado *a la creación de buenas prácticas como medida de protección de la información en las compañías aseguradoras* que trabajan las distintas opciones de seguro de personas, tal es el caso de los seguros de vida, los seguros de accidentes y los seguros de enfermedades, la razón por la cual está dirigido a este tipo de organización es debido a que en México aún no se cuenta con una ley claramente definida para la protección de información sensible como lo son los datos personales y que son la fuente principal de información de las compañías aseguradoras para integrar los expedientes de los candidatos a obtener el seguro, cabe mencionar que se cuentan con iniciativas para la modificación de artículos de la Constitución Política de los Estados Unidos Mexicanos *(6, 16 y 73)* y con actividades a cargo del IFAI *(Instituto Federal de Acceso a la Información Pública)*, lo cual representa un gran avance para generar un respaldo legal en este ámbito de protección.

Es importante que las compañías aseguradoras, como entidades proveedoras del servicio de seguridad a sus clientes y regidas bajo el principio de transferencia de riesgo, puedan garantizar que cumplen con los controles de seguridad dentro y fuera de sus instalaciones para la protección de la información a su cargo y de esta forma evitar se presente algún tipo de daño cuyas consecuencias generarían desde daño en el prestigio, pérdidas económicas hasta el cierre de la organización.

Este trabajo representa una innovación debido a la importancia del tema que aborda, ya que funge como una base para futuras investigaciones que mejoren la forma en la cual es protegida la información en las compañías aseguradoras.

Siendo esto un buen principio que muestra cómo los conceptos de la seguridad informática son aplicados en la creación de buenas prácticas que contribuyan a regular la forma en la cual las compañías aseguradoras almacenan, manipulan y transmiten la información confidencial de sus clientes.

El desarrollo de este trabajo inicia con la definición de conceptos básicos en el ámbito de la seguridad informática que permiten colocar en contexto al lector con los términos, que serán utilizados a lo largo del texto.

En el *segundo capítulo* se definen y aplican los conceptos relacionados con los criterios comunes y el perfil de protección enfocados en la protección de la información confidencial en las compañías aseguradoras.

En el *tercer capítulo* se establecen los estándares y leyes actuales tanto a nivel internacional como en México que están dedicados a la protección de la información.

El *cuarto capítulo* define la importancia de la criptografía como herramienta para que las compañías aseguradoras protejan la información confidencial de sus clientes, en esta parte se especifican los diferentes métodos de cifrado, sus ventajas y desventajas.

Por último, en el *quinto capítulo* se define el conjunto de buenas prácticas, las cuales consideran un escenario general con relación a la manipulación de la información por las compañías aseguradoras y tienen por objetivo poder ser aplicadas y ajustadas de forma particular considerando las necesidades y requerimientos de cada compañía.

CAPÍTULO 1

Seguridad informática

"Fiarse de todo el mundo y no fiarse de nadie son dos vicios: pero en el uno se encuentra más virtud, y en el otro más seguridad"

SÉNECA, Lucio Anneo

1.1 Seguridad.

La importancia que posee la protección de los bienes radica en qué tan necesarios o valiosos sean para los propietarios o personas encargadas de la manipulación de los mismos y para ello surge la necesidad de definir el concepto sobre el cual se sustenta el desarrollo del presente trabajo.

a) Definición.

La palabra ***seguridad*** tiene un origen etimológico del latín "securitas"[1], que significa "Cualidad de seguro", partiendo de este concepto se define la seguridad como el conjunto de medidas implementadas para la protección de los activos de agentes que puedan representar un riesgo para los mismos. Analizando el sujeto de estudio en esta definición, se identifica que el activo más importante, después de los recursos humanos dentro de una organización es la *información*, la cual está constituida por un conjunto de *datos*[2] previamente analizados y que debido a ello adquieren un determinado valor, ésta es la razón por la cual surgen conceptos relacionadas con la seguridad para salvaguardar la información tales como, la *seguridad informática*, la *seguridad de la red* y la *seguridad de la información*, los cuales se ilustran en la figura 1.1 y serán definidos a continuación:

Figura 1. 1 Esquema de la seguridad aplicada a la información.

[1] http://es.wiktionary.org/wiki/seguridad

[2] **Datos:** Conjunto de caracteres, letras números que no tienen significado alguno, debido a que no han sido sujetos a ningún análisis

- ✓ Seguridad informática: este término hace referencia al conjunto de herramientas creadas con el objeto de brindar protección a los activos y con ello evitar que personas no autorizadas, interfieran en el funcionamiento adecuado de un determinado sistema de cómputo. Se encarga de proteger a los sistemas informáticos de amenazas que interfieran o dañen los servicios de seguridad como son la confidencialidad, integridad y disponibilidad.

- ✓ Seguridad de la Red: como consecuencia del crecimiento de la tecnología y las necesidades de la comunicación e intercambio de información entre usuarios, así como también las organizaciones, surge la necesidad de la interconexión de equipos informáticos para compartir recursos e información, es decir, la creación de redes y para la protección de éstas, surge la seguridad de la red, la cual se encargará de la protección de información, recursos y servicios, de todo aquello que pueda representar una amenaza contra los mismos.

- ✓ Seguridad de la información: está relacionada con las medidas implementadas para la prevención y protección de la información, de daños como la modificación, el robo, la revelación a personal no autorizado y la destrucción.

La figura 1.2, ilustra los diferentes enfoques de la seguridad y sus ámbitos de aplicación.

Figura 1. 2 Seguridad y sus diferentes enfoques.

b) Ventajas y desventajas.

El proveer seguridad en la información manejada por una organización, conlleva una serie de ventajas y desventajas las cuales se describen a continuación (Tabla 1.1), en ellas se puede observar los beneficios que se obtendrían dentro de la organización, pero a su vez el precio que tendría que pagarse por implementar las herramientas proveedoras de seguridad.

Tabla 1. 1 Relación de ventajas y desventajas al implementar herramientas que proporcionen seguridad informática dentro de una organización

Ventajas	Desventajas
✓ Disminución de las vulnerabilidades de los activos que posee la organización. ✓ Se protege la información confidencial, de posibles ataques o de usuarios no autorizados para tener acceso a ella. ✓ Menos costoso el proteger la información en relación a la pérdida de la misma. ✓ Se adquiere un conocimiento más amplio de los posibles daños que podría tener la información manipulada y almacenada por la organización.	✓ Si no se cuenta con una capacitación adecuada, podría no conseguirse el objetivo de protección deseado. ✓ Resulta costosa, si el diseño previo y la implementación fueron mal elaborados. ✓ La implementación excesiva de herramientas proveedoras de seguridad, podría convertir a un sistema informático en incompetente para poder realizar el trabajo, para el que fue diseñado. ✓ Algunos métodos de cifrado implementados para la protección de la información, resulta costosa su implementación en hardware, lo que se convierte en una mayor inversión económica para una organización.

c) Herramientas de seguridad.

Para poder lograr la seguridad de la información dentro de una organización, es necesario determinar las herramientas que serán empleadas para dicho objetivo, razón por la cual se debe dar respuesta a tres interrogantes que permitirán seleccionar las herramientas adecuadas que la organización requiere para proveer seguridad. Las cuales deben ser formuladas en dicho orden, de esta forma al obtenerse las respuestas, se identifican tanto los activos de la organización, así como las amenazas y vulnerabilidades a las cuales están expuestos y con base en esto, se fijarán las posibles

herramientas que darán solución a los problemas de seguridad informática planteados (Figura 1.3).

Figura 1. 3 Cuestionamientos necesarios para la elección de herramientas de seguridad

Los cuales se mencionan a continuación:

- ✓ ¿Qué se desea proteger?

  Este cuestionamiento tiene por objeto la identificación de los activos dentro de la organización, es decir todo aquello que se quiere proteger y con ello se determina el entorno de seguridad[3], identificando a su vez los riesgos de los que podrían ser objeto esos bienes y las consecuencias que implicaría el daño en la disponibilidad, la integridad y la confidencialidad de los mismos.

- ✓ ¿De qué se desea proteger?

  Dando respuesta a este cuestionamiento se identifican las amenazas, las vulnerabilidades y los riesgos del entorno de seguridad previamente identificado, de esta forma se reconocen los actores principales que ponen en riesgo la seguridad de los activos, lo que permitirá definir el escenario de estudio y a su vez la selección de las herramientas requeridas para proveer de seguridad una organización.

- ✓ ¿Cómo lograr protegerlo?

  Para contestar esta interrogante es necesario que las preguntas anteriores estén claramente definidas, pues de esto dependerán las soluciones

[3] **Entorno de seguridad:** delimitación del área que contiene los activos que requieren protección de intrusos o agentes que puedan dañarlos.

propuestas y las herramientas empleadas para salvaguardar los activos de todo aquello que pueda dañarlos, además algunas de las soluciones posibles serían el apego a estándares internacionales que permitan la creación de políticas de seguridad informática, que regulen la forma en la cual serán manipulados los activos dentro de una organización, permitiendo así la disminución de las vulnerabilidades y amenazas que pongan en riesgo a la misma.

1.2 Riesgos y amenazas

La exposición constante de los activos, debido a la manipulación de éstos en una organización, incrementa los riesgos y las amenazas a las cuales pueden estar expuestos, razón por la cual es importante se tengan los conocimientos relacionados con el tipo de riegos y amenazas existentes, lo que permitirá tomar determinadas medidas de protección con base en los riesgos y amenazas identificados dentro del entorno de seguridad.

a) Definición.

La palabra *riesgo* hace referencia a la posibilidad de ocurrencia de una *amenaza*, definiendo ésta como aquello que pretende causar algún daño o destrucción.

b) Niveles de riesgos.

Los riesgos pueden clasificarse con base en dos criterios, lo cuales se muestran en la figura 1.4, donde uno de ellos está relacionado con el nivel de importancia de los recursos y otro con la severidad de su pérdida.

- Estimación del nivel de importancia del recurso.
- Estimación del riesgo de la pérdida del recurso.

Para cuantificar dichos niveles es posible asignar valores numéricos en una escala de 0 a 10, que permitan identificar los recursos de mayor importancia con el número 10 y a su vez el riesgo de perderlo, considerando como 10, cuando se tiene el riesgo más alto.

Figura 1. 4 Niveles de riesgos

c) Clasificación de las amenazas.

Como parte del conocimiento requerido para la protección del entorno de seguridad, se encuentran las cinco fuentes principales de amenazas, las cuales se mencionan en la tabla 1.2.

Tabla 1. 2 Tipos de amenazas.

TIPO DE AMENAZA	DESCRIPCIÓN
De tipo lógico	Este tipo de amenazas está relacionado, con una inadecuada implementación de mecanismos de seguridad en un sistema determinado, lo cual es aprovechado por los códigos maliciosos[4].
De humanos	Estas amenazas se presentan cuando existen: • Descuidos • Negligencias • Inconformidades. • Ignorancia Con la información que es manejada por los usuarios dentro de una organización. Debido a que existen diferentes tipos de ataques, así como variantes en las técnicas empleadas, dichos personajes ejecutores reciben diferentes nombres tales como, *hackers*, *crackers*, *bucaneros*, *newbie*, *phreaker*, *lamers*, *scriptkiddie*,

[4] **Código malicioso:** Software que accede a un sistema de cómputo, sin autorización intentando violar las reglas previamente establecidas hasta lograr comprometerlo. Para más información ver apéndice A

	spammers, *trashing*, de los cuales se detalla su definición en el Apéndice B.
Errores de hardware	Se presentan amenazas de este tipo cuando hay fallas físicas en los dispositivos de hardware.
Errores de la red	Surgen como consecuencia de un mal diseño e implementación de la red, lo que ocasiona que el flujo de la información dentro de la organización no sea el óptimo o el requerido.
Naturales	Este tipo de amenazas, se presentan debido a las acciones de la Naturaleza, tales como las inundaciones, los terremotos, los incendios, los fuertes vientos, factores que influyen en el bienestar físico de los sistemas de cómputo y en general de las organizaciones.

1.3 Vulnerabilidades

La presencia de ataques dentro de las organizaciones, es debido a las vulnerabilidades existentes dentro de las mismas, esto conlleva a definir dicho término, así como también mostrar una clasificación de los tipos de vulnerabilidades que pueden presentarse.

a) Definición.

Una *vulnerabilidad* es toda aquella situación que pueda tener como consecuencia un problema de seguridad, a su vez también está definida por puntos susceptibles en un sistema, los cuales pueden ser blanco fácil, para ser explotados por los perpetradores, comprometiendo la seguridad del mismo y en casos más drásticos de la organización.

Un punto susceptible en un sistema se considera como aquella área que se encuentra expuesta a ataques que atenten contra la seguridad, como por ejemplo la búsqueda del acceso al sistema por parte de un intruso, la obtención de información sensible con fines maliciosos, el daño o entorpecimiento de las actividades realizadas por el sistema víctima, el conseguir privilegios para modificación o robo de información, entre otros.

b) Clasificación.

Con base en la definición anterior, se enlistan a continuación, en la tabla 1.3, los tipos de vulnerabilidades existentes.

Tabla 1. 3 Tipos de vulnerabilidades

TIPO DE VULNERABILIDAD	DESCRIPCIÓN
Física	Este tipo de vulnerabilidad hace referencia al control de acceso físico al sistema, es decir qué tan posible es el acceder físicamente al sitio donde éste se encuentra localizado y con qué facilidad puede ser víctima de algún tipo de daño, robo o destrucción.
Natural	Esta vulnerabilidad se refiere al grado en que un sistema puede afectarse como consecuencia del impacto de algún desastre natural, tales como (inundaciones, terremotos, lluvias eléctricas, etcétera). Ejemplo de la presencia de dichas vulnerabilidades, sería el no considerar medidas de protección de los activos, como el resguardo de equipos de cómputo y respaldo de la información, en otra ubicación alejada de la organización como medida de protección contra las inundaciones, la falta de condiciones adecuadas en las instalaciones o la proximidad del área con zonas que representen una cierta peligrosidad de incendios, o percances que pongan en riesgo los activos de la organización.
De software	Se refiere a las fallas o debilidades existentes en los programas de un sistema que facilite las labores de intrusión al mismo, ejemplo de ello son los errores de programación en aplicaciones propias o ajenas al sistema operativo, que comprometan el sistema y lo expongan a la detección de más vulnerabilidades y a la explotación de las mismas.
De hardware	Ésta se presenta cuando no se tienen las precauciones necesarias, con los equipos de hardware, ejemplo de ello, el no verificar las indicaciones descritas en los manuales de operación de los dispositivos, lo que ocasionaría una mala instalación o manipulación del mismo y en el peor de los casos el daño de éste, otro de los puntos que podrían ocasionar una vulnerabilidad de este tipo, es la falta de mantenimiento en los dispositivos de hardware o el mal uso al que pueda ser sujeto por parte los usuarios.

De red	Considerando la creciente necesidad de compartir e intercambiar, información, comunicación y recursos entre equipos y organizaciones a nivel nacional e internacional, surgen las redes de computadoras, pero ello conlleva a un incremento en el riesgo a sufrir ataques, como consecuencia de la explotación de las vulnerabilidades, detectadas en las redes, que surgen en la mayoría de los casos, por una mala estructuración de la red, errores de diseño en el cableado estructurado, deficiencias en la administración, lo cual será un blanco fácil para los intrusos y con ello los hosts vulnerados serán puertas de acceso hacia el sistema que controla la red, ocasionando un problema de seguridad dentro de la organización.
Humana	Esta vulnerabilidad está relacionada con los errores que puedan presentarse como producto de descuidos del personal, es decir, qué tan susceptibles sean éstos a la aplicación de técnicas de ingeniería social o ingeniería social inversa para obtener información confidencial, además de las medidas que considere la organización para la selección de su área de recursos humanos y la forma de comunicación con los mismos, para evitar malos entendidos que desencadenen problemas en las actividades que realizan y que pongan en riesgo la confidencialidad, integridad y disponibilidad de los activos empleados por la organización.

1.4 Ataques

Una vez detectadas las vulnerabilidades en una organización, existen dos caminos para proceder, el positivo, en el cual se provocan ataques como prueba con el objeto de detectar el impacto y las vulnerabilidades y con ello disminuir los problemas de seguridad, por otro lado, el camino negativo está orientado a la generación de ataques con fines maliciosos, para el robo o modificación de la información, o el daño del sistema para generar una denegación de servicio[5]. Debido al impacto que tienen en las organizaciones, a continuación se explica el concepto, metodología y clasificación de los ataques.

[5] **Denegación de servicio:** término que por sus siglas en inglés se denomina DOS (Deny of Service), el cual hace referencia al tipo de ataque, que consiste en la imposibilidad de acceso a un recurso o servicio por parte del usuario legítimo.

a) Definición.

Un *ataque* es definido como la explotación por medio de una amenaza, de una vulnerabilidad detectada. Es la culminación de una amenaza al explotar una o varias vulnerabilidades.

b) Etapas que constituyen un ataque.

El camino para la ejecución de un ataque, está formado por tres etapas principales, donde cada una de ellas se encargará de dar respuesta a una de las siguientes tres interrogantes planteadas:

- ¿Qué se desea realizar?
- ¿Cómo se llegará al objetivo deseado?
- ¿Se ha logrado el objetivo y qué se obtuvo al llevarse a cabo?

Una vez definidas las interrogantes que serán el punto de partida para cada una de las etapas que integran un ataque, éstas serán explicadas a continuación y se ilustran en la figura 1.5:

✓ Preparación y planteamiento:

Esta parte es la encargada de la recolección de la información necesaria para tener un panorama amplio del blanco víctima, para realizar dicha labor, se emplean técnicas como, ingeniería social, información en Internet, uso de aplicaciones de tipo *key loggers*, *phishing*, *sniffers*, libros, documentos, o fotocopias que arrojen información de importancia. Mediante el uso de diversas herramientas, esta etapa dará respuesta al cuestionamiento, ¿Qué se desea realizar?, dejando claramente definido el objetivo del ataque.

✓ Activación:

En esta etapa se contemplan todos los recursos físicos y lógicos que son empleados para la obtención del objetivo, definido anteriormente. La respuesta que se obtendrá como resultado en esta etapa es a la pregunta ¿Cómo se llegará al objetivo deseado?, para ello se puede hacer uso de bombas

de tiempo, las cuales esperaran la ejecución de un proceso para realizar la activación de una bomba lógica[6].

✓ Ejecución:

Esta etapa contempla todo aquello relacionado con los resultados obtenidos al efectuar el ataque, es decir, si se logró el fin determinado en etapas anteriores, si los medios para conseguirlo fueron los adecuados y finalmente lo que se obtuvo del ataque realizado, ya sea una denegación o robo del servicio, conocimiento o modificación de información, acceso a recursos o sistemas, etcétera.

Figura 1. 5 Etapas de un ataque

c) Clasificación.

Esta clasificación está determinada con base en el impacto del ataque sobre los activos.

✓ Ataques pasivos:

En este tipo de ataques, el atacante no modifica la información, únicamente realiza tareas como, la observación, el monitoreo y el escuchar con detenimiento mientras la información está siendo transmitida, dentro de los principales objetivos de este tipo de ataque destacan, la intercepción de datos y el análisis de tráfico.

[6] **Bomba lógica:** es un programa informático que se instala en un equipo, permaneciendo oculto, hasta cumplirse condiciones determinadas para su activación y con ello ejecutar las acciones para las cuales fue creada.

La información que puede obtenerse mediante ataques pasivos es:

- *Obtención de la identidad de emisor y receptor*:

  Esto hace referencia a las labores del intruso mediante la lectura de las cabeceras de los paquetes que son transmitidos en la red con el objeto de identificar quién envía y quién recibe dicha información.

- *Control del volumen de tráfico y de las horas de intercambio de datos.*

  Mediante esta técnica de ataque, se observan la frecuencia de las actividades realizadas por la organización, conociendo los días y horas en los cuales se presenta la mayor actividad y con un estudio a detalle es posible determinar los momentos en los cuales se hace el manejo de información sensible para la organización.

Otra característica de este tipo de ataque es que su detección e intercepción es complicada, debido a que no hay alteración de la información y no hay forma de percibir la presencia de dicho ataque.

Como una alternativa, para evitar ser blanco de este tipo de ataques, se puede recurrir a la implementación de técnicas de cifrado.

✓ Ataques activos:

En los ataques de este tipo, se presenta modificación de la información, interrupción en un determinado servicio, a diferencia de los ataques pasivos, éstos sí pueden ser detectados por el impacto que ocasionan dentro de la organización, aunque la mayoría de las veces resulta tarde la detección de los mismos.
Este tipo de ataques pueden clasificarse, tal como se muestra en la tabla 1.4

Tabla 1. 4 Clasificación de ataques activos.

TIPO DE ATAQUE ACTIVO	DESCRIPCIÓN
Modificación de mensajes	En este tipo de ataque se cuenta inicialmente con un mensaje original, el cual es modificado en una parte de forma no autorizada, lo que ocasiona que la integridad del documento se vea alterada.

Réplica y reactuación	En este caso se cuenta con un mensaje legítimo, el cual es interceptado y repetido con una modificación previa y después de ello se realiza una retransmisión del mismo en diversas ocasiones. Ejemplo de este tipo de ataque podría ser, el ingreso en una cuenta bancaria dinero en repetidas ocasiones.
Suplantación de identidad	Mediante este ataque el intruso suplanta a una entidad diferente con el objeto de conseguir acceder a recursos que están disponibles únicamente para usuarios con privilegios.

1.5 Servicios de seguridad

a) Definición.

Es aquel que permite mejorar la seguridad tanto en un sistema de información como el flujo de la misma en una organización. Están destinados a evitar ataques de seguridad y emplean uno o muchos elementos de seguridad para brindar el servicio.

b) Clasificación.

Los servicios de seguridad son seis, los cuales se describen en la tabla 1.5.

Tabla 1. 5 Servicios de seguridad.

CONFIDENCIALIDAD	Que sólo tenga acceso a la información la persona autorizada.
Ejemplos: ✓ Contraseñas para el inicio de sesión en una PC, para que la información contenida en ella sólo sea accedida por el usuario indicado o por el propietario. ✓ Candados y cerraduras en algún lugar que resguarde información importante. ✓ Que una contraseña sólo sea conocida por el propietario de la misma.	
AUTENTICACIÓN	Consiste en verificar la identidad de la persona que desea acceder a la información.

Ejemplos:

- ✓ Autenticación por medio de la credencial de elector para hacer el cobro de un cheque en un banco.
- ✓ Lector de huellas digitales para identificar a las personas.
- ✓ Identificación a nivel del ADN de una persona para determinar el parentesco.

INTEGRIDAD	Observar que los datos se encuentren sin ninguna alteración visible.

Ejemplos:

- ✓ Cuando se recibe un paquete se verifica que no estén alterados los sellos o esté abierto.
- ✓ Cuando se compran vinos y se verifica que tenga el sello de la SHCP que avale la autenticidad del producto y además que éste no éste adulterado.

NO REPUDIO	Permite la protección entre usuarios por si alguno de ellos negara, una comunicación ya sea de envío o de recepción.

Ejemplos:

- ✓ En las inscripciones y cuando un usuario ya realizó su inscripción previamente, el servidor detecta esto y le impide que fuera de su horario y pasado su tiempo vuelva a modificar la inscripción realizada con anterioridad, pues hay un antecedente de que ya previamente hizo un trámite, es decir, había una conexión previa que el alumno no puede negar.

CONTROL DE ACCESO	Es la habilidad para permitir o denegar el acceso a las aplicaciones y sistemas, su finalidad es que el usuario tenga el acceso autorizado cuando ha pasado previamente por una etapa de identificación y otra de autentificación.

Ejemplos:

- ✓ El NIP de las tarjetas de débito o crédito cuando se realiza alguna transacción a través de los cajeros automáticos, es el control de acceso a la información y movimientos de una cuenta bancaria.
- ✓ La credencial de la UNAM que permite el acceso al estacionamiento, el código de barras de la credencial pasará por una etapa de identificación, de autentificación y permitirá el acceso.

DISPONIBILIDAD	La información debe estar disponible, las veces que sea necesario, para cuando los usuarios autorizados la requieran.

Ejemplos:

- ✓ En una base de datos por ejemplo, en un banco se debe tener la información de los cuentahabientes en cualquier momento.
  En un supermercado se debe tener siempre disponible la información que relaciona los códigos de barras de los productos con el precio correspondiente.

CAPÍTULO 2

Criterios comunes y perfil de protección

"La mejor forma de predecir el futuro es implementarlo"
HEINEMEIER, Hansson David

2.1 Criterios comunes

Mediante dos componentes clave, los cuales son los perfiles de protección y la evaluación de niveles de seguridad, los criterios comunes contribuyen con la identificación de las necesidades de seguridad que deben cubrir los productos y sistemas además de la evaluación una vez que han sido implementadas.

a) Definición

Los *Criterios Comunes para la evaluación de seguridad de tecnología de la información (Common Criteria for Information Technology Security*) mejor identificados como CC, fueron creados con base en criterios europeos, norteamericanos y canadienses por lo cual se definen como una norma internacional cuyo objetivo principal es la protección de la información mediante evaluaciones de seguridad, de los productos relacionados con las tecnologías de la información. Estas evaluaciones se realizan mediante una autoridad específica la cual deberá seguir lo establecido en los CC reconocidos a nivel mundial.

- Historia

Los CC tienen como antecedente dos importantes criterios de evaluación, tal como se muestra en la figura 2.1, los cuales son:

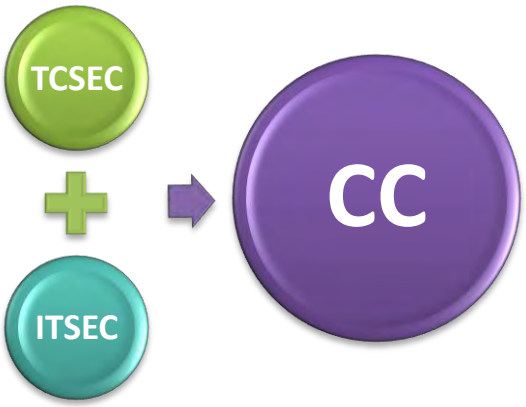

Figura 2. 1 Antecedentes de los Criterios comunes.

- ✓ TCSEC *(Trusted Computer Security Evaluation Criteria or Orange Book)- Criterio de Evaluación de Seguridad de Computo Confiable.*

Los *TCSEC* conocidos como libro naranja, fueron creados a mediados de los años ochenta por el Departamento de Defensa (DoD)[1], con el objeto de evaluar la seguridad y de tener una medición confiable de la misma, se preocupa por el mantenimiento de la confidencialidad de la información clasificada a nivel nacional.

En un entorno particular resultaba conveniente el uso de los TCSEC, debido a que éstos proveían niveles que requerían una funcionalidad de seguridad específica.

El libro naranja define cuatro divisiones jerárquicas de seguridad para la protección de la información, las cuales se muestran en la figura 2.2 y se definen a continuación:

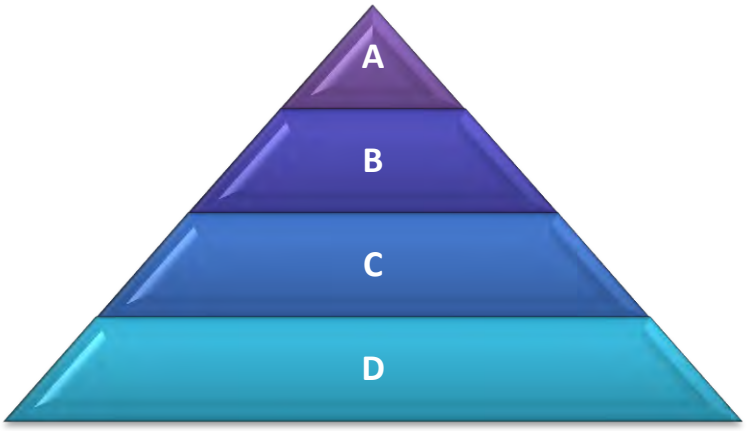

Figura 2. 2 Divisiones jerárquicas de seguridad: A Protección controlada, B Protección obligatoria, C Protección discrecional, D Protección Mínima

A *Protección controlada:* Emplea métodos formales para llevar a cabo verificaciones de seguridad garantizando con ello que los controles de seguridad obligatoria y discrecional empleados en el sistema, sean capaces de proteger de forma eficiente la información clasificada o sensitiva que es procesada o almacenada por el sistema evaluado.

[1] **DoD** Department of Defense: (Departamento de Defensa de los Estados Unidos).

***B** Protección obligatoria:* contiene tres clases B1, B2 y B3, donde ésta última ofrece mayor seguridad. Un requisito importante en esta división es preservar la integridad de etiquetas de sensibilidad de la información, las cuales se utilizan para cumplir el conjunto de reglas obligatorias del control de acceso.

***C** Protección discrecional:* este tipo de división está definida como la necesidad de identificación y que mediante capacidades de auditoría exige a los usuarios responsabilizarse de las acciones realizadas. Contiene dos distintas clases C1 y C2 donde la segunda ofrece una mayor seguridad.

***D** Protección mínima:* esta división está constituida por una clase y es empleada para sistemas que una vez evaluados, no cumplen con los requisitos para pertenecer a una clase más alta de evaluación. Ejemplo de este tipo de sistemas es el DOS[2] para computadoras personales.

- ✓ ITSEC *(Information Technology Security Evaluation Criteria)- Criterio de Evaluación de la Seguridad de las Tecnologías de la Información,* por los gobiernos de Francia, Alemania, Reino Unido y Holanda.

Fueron creados a principios de los años noventa, proveía niveles de seguridad mediante los cuales definían la funcionalidad del producto desarrollado.

Los ITSEC poseen siete niveles de evaluación E0, E1, E2, E3, E4, E5 y E6, donde éste último representa una posibilidad mayor por alcanzar la meta u objetivo de seguridad mientras que E0 represente una menor posibilidad.

El proceso de evaluación tiene por objetivo permitir al evaluador preparar un informe imparcial, mediante el cual indique si el sistema, que es sujeto de estudio satisface o no su meta de seguridad de acuerdo con el nivel de confianza precisado por el nivel de evaluación.

b) Estándar ISO/IEC 15408

A finales de año 1998 surge un nuevo esquema para evaluar la seguridad remplazando al TCSEC y ITSEC, logrando con ello la creación de lo que actualmente es conocido como Criterios Comunes.

[2] **DOS** Disk Operating System: Sistema Operativo de Disco, utilizado por las computadoras personales.

- Historia

El esquema creado es el resultado de proyectos cooperativos, los cuales tenían una relación con la Organización Internacional de Estándares (ISO), debido a que el contenido de la versión 2.0 de CC era similar a la redacción final del Comité (FCD) 15408 ésta fue llevada ante la ISO, lo cual una vez aceptada por ésta, daría como resultado en diciembre de 1999 el *CCITSE versión 2.1, "Tecnología de Información- Técnicas de seguridad- Criterios de evaluación para la seguridad de IT" (ISO-IEC 15408)*, los cuales sustituyen al libro naranja y son empleados para seguir niveles de seguridad determinados.

El objetivo de que ISO adoptara el CCITSE versión 2.1, radica en la necesidad de tener un criterio encargado de la evaluación de la seguridad en productos relacionados con tecnologías de la información el cual fuera reconocido internacionalmente, creando de esta forma metodologías estándar que permitan satisfacer las necesidades (en materia de seguridad) de los consumidores, desarrolladores y evaluadores.

La aprobación internacional de los CC es un cambio representativo para el gobierno y la industria relacionada con las tecnologías de la información además de los perfiles de protección de las evaluaciones de seguridad.

Dentro de la evaluación de las propiedades de seguridad de los productos intervienen tres grupos, los cuales se encuentran representados mediante la figura 2.3.

Figura 2. 3 Grupos que intervienen en la evaluación de las propiedades de seguridad de los productos.

- ✓ *Consumidores:* usan los resultados de las evaluaciones de seguridad para decidir si el producto o sistema satisface sus necesidades de seguridad.

- ✓ *Desarrolladores:* los CC proveen una serie de criterios, los cuales están diseñados de tal forma que les permitan cubrir requerimientos de seguridad en niveles diferentes basados en lo que requieran los consumidores.

- ✓ *Evaluadores:* los criterios comunes proporcionan aspectos de seguridad de los productos TI, que deben cubrir los desarrolladores y que son medidos de manera respetable, reproducible e independiente, lo cual permitirá asegurar que los resultados obtenidos en la evaluación sean verídicos y determinen el nivel de seguridad con el cual han sido desarrollados los productos. Con la finalidad de que los consumidores puedan asegurar que sus requerimientos de seguridad han sido considerados y cubiertos por los desarrolladores.

- Estructura ISO/IEC 15408

El estándar engloba una serie de métodos para evaluar los niveles de seguridad de productos TI, está integrado por tres partes que se encuentran claramente definidas mediante la tabla 2.1.

Tabla 2. 1 Partes del ISO/IEC 15408

Nombre	Descripción
Introducción y modelo general	En esta parte se encuentran contenidas las estructuras y descripciones de los *Perfiles de Protección "Protection Profiles"* y *los Objetivos de o metas de Seguridad "Security Targets"*, los cuales son usados para la definición de los grupos específicos de las necesidades de seguridad para los productos y sistemas, además de la descripción de cómo fueron establecidos los CC y para quiénes están destinados
Requerimientos funcionales	Esta parte tiene como destino los usuarios y desarrolladores, ya que establece un conjunto de componentes funcionales de seguridad como estándar que permiten expresar los requerimientos de seguridad funcional para los

	productos y sistemas. Estos requerimientos están organizados en once clases que reciben el nombre de *"Clases de requerimientos funcionales"*, las cuales a su vez se encuentran divididas en una o más familias funcionales.
Requerimientos de garantía	Esta parte está destinada a los desarrolladores ya que en ella se encuentra definido el criterio de la confiabilidad que los evaluadores emplean para verificar el desempeño de los desarrolladores y sus productos. Se cuenta con siete niveles de evaluación de garantía (Evaluation Assurance Level EAL), los cuales son empleados como escala para clasificar la evaluación obtenida por los productos.

c) Beneficios

Las ventajas que ofrecen los CC benefician tanto a los consumidores como a los desarrolladores de productos de tecnologías de la información.

- ✓ *Para los consumidores:* los CC proveen medios de comparación entre los diferentes productos ofrecidos por los desarrolladores además los consumidores crean esquemas en los cuales plantean sus necesidades de seguridad, lo que permite a los desarrolladores entender de forma clara y concisa lo que los consumidores requieren.

  El uso de productos evaluados por criterios internacionales y reconocidos incrementa en los consumidores la confiabilidad en la funcionalidad relacionada con la seguridad de los productos TI.

- ✓ *Para los desarrolladores:* Los CC proporcionan una ventaja competitiva en los productos, esto lo hacen mostrando a nivel mundial que un producto cumple las expectativas esperadas en el ámbito de la seguridad.

2.2 Perfil de protección

Un perfil de protección *PP (Protection Profile)* está conformado por un conjunto de requerimientos de seguridad, los cuales pueden ser los establecidos en los Criterios Comunes o indicados de forma explícita. Fueron creados con el objeto de presentar de forma rigurosa un determinado problema de seguridad y los requerimientos necesarios para la solución del mismo.

a) Definición

Es un documento mediante el cual se diseña un esquema de seguridad, es decir, es un conjunto estándar de requerimientos de seguridad los cuales deben satisfacer los productos y sistemas de una organización con el objetivo de responder a las necesidades en el ámbito de la seguridad informática planteadas con los consumidores de TI.

Un PP debe ser redactado considerando que es un documento orientado al usuario y se tienen que definir los requisitos útiles y eficaces para el cumplimiento de los objetivos identificados, con la finalidad de resolver el problema de seguridad.

El propietario de la organización o el titular de la misión es la primera persona que da lectura al perfil de protección considerando que es un documento de gran utilidad tanto para los consumidores, desarrolladores y evaluadores ya que todos interactúan en las actividades que darán solución al problema especificado.

b) Elementos que lo conforman

Un evaluador basado en los fundamentos establecidos en los CC establece un criterio para determinar si un PP cumple con las características requeridas (completo, consistente y válido técnicamente) y con base en ello toma la decisión de presentarlo como un informe de requerimientos para un entorno de seguridad.

La importancia de dicha metodología es debido a que ésta define los requerimientos de los consumidores, así como una descripción clara del panorama de acción, lo cual permitirá que los productos desarrollados o seleccionados cumplan con las necesidades requeridas por el objeto de evaluación, logrando con ello una solución óptima al problema de seguridad planteado.

La estructura que se muestra en la figura 2.4 corresponde a la metodología de perfiles de protección, se encuentra constituida por seis etapas, las cuales serán explicadas a continuación:

Figura 2. 4 Estructura metodología perfiles de protección

- Introducción al PP

Esta etapa tiene como objetivo proporcionar un resumen de carácter ejecutivo, que es la información que será dirigida al directivo de la organización, la cual deberá estar redactada de forma clara y concisa, planteando el problema de seguridad detectado, mediante la presentación de un esquema que permita llegar a una solución óptima y satisfactoria.

Dos partes importantes que integran esta etapa se muestran en la figura 2.5:

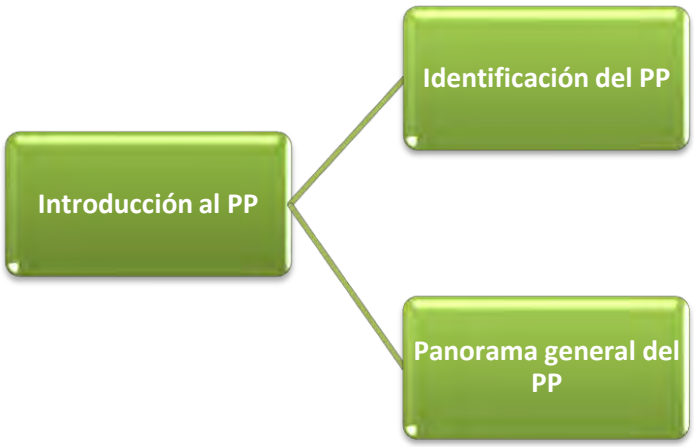

Figura 2. 5 Partes que integran la introducción al PP

- ✓ *Identificación del PP:* consiste en información descriptiva que permitirá identificar, registrar y clasificar un PP.

- ✓ *Panorama general:* es una recopilación de forma narrativa en la cual se plantea a detalle el panorama con la finalidad de que los lectores mediante la introducción determinen si el PP descrito es de interés para la organización.

- Descripción del objeto de evaluación

En esta etapa se definen los requerimientos de seguridad del objeto de evaluación, información que será utilizada en el transcurso de la evaluación para permitir identificar las inconsistencias que existen si es que las hay, de esta forma también se añaden detalles que enriquezcan la información previamente definida en la introducción.

Debe incluir una descripción funcional detallada, considerando que ésta será leída principalmente por el técnico administrador, en la cual se debe mostrar claramente la

descripción de la frontera del objeto de evaluación definido y lo que queda fuera de éste.

- Entorno de seguridad del objeto de evaluación

Consiste en realizar una descripción del entorno en el cual se tiene contemplado usar el objeto de evaluación y la forma en la cual será empleado, considerando todos los aspectos de seguridad que sean posibles.

Esta etapa debe incluir tres aspectos principales mostrados en la figura 2.6.

Figura 2. 6 Partes que integran el entorno de seguridad del objeto de evaluación

- ✓ *Hipótesis:* menciona cómo será usado el objeto de evaluación (la aplicación, el valor de los bienes potenciales y las limitaciones de su uso), además de información relacionada con su entorno considerando los aspectos físicos, personales y de conectividad entre sujetos y objetos. Se deberá plantear una hipótesis que haga referencia al comportamiento de forma segura que deberá tener el objeto de evaluación, también deberán estar definidos los alcances de los requerimientos y evitar proporcionar detalles de las funciones de seguridad.

- ✓ *Amenazas:* consiste en la definición de todo aquello que se considere pueda dañar o destruir los bienes de la organización, en esta parte se deben describir los agentes de amenaza basándose en la experiencia, los

recursos disponibles y la motivación, por otra parte, deben ser mencionados los ataques, es decir los métodos utilizados, las vulnerabilidades explotadas y la oportunidad.

- ✓ *Políticas de seguridad informática de la organización:* hace referencia a la definición de políticas que puedan ser implementadas por el objeto de evaluación.

- Objetivos de seguridad

En esta etapa se establecen los objetivos de seguridad para el objeto de evaluación y su entorno considerando todos los aspectos de seguridad identificados, reflejando de esta forma el estado del proyecto.

Los objetivos de seguridad definirán la forma en la cual se hará frente a las amenazas y políticas desde el punto de vista de la hipótesis además de la naturaleza de los requerimientos, enfoque particular de cada objetivo y la relación entre el objetivo, las políticas y las amenazas.

Dentro de esta etapa se encuentran comprendidos, los objetivos de seguridad para el objeto de evaluación y para el entorno tal como se muestra en la figura 2.7.

Figura 2. 7 Partes que integran los objetivos de seguridad

- ✓ *Para el objeto de evaluación:* deberán estar claramente documentados y deben hacer referencia a las amenazas identificadas que serán contrarrestadas por el objeto de evaluación y por las políticas de la organización.

- ✓ *Para el entorno de seguridad:* se refiere a las amenazas identificadas y que no han sido contrarrestadas por el objeto de evaluación y las políticas de seguridad de la organización o hipótesis reunidas de forma incompleta.

Para determinar los objetivos de seguridad se deben considerar los siguientes pasos:

- ✓ Se lleva a cabo un primer análisis considerando los resultados obtenidos del análisis del entorno de seguridad, esto es, considerando la hipótesis, las amenazas y las políticas de seguridad.

- ✓ Mediante un segundo análisis y con base en los resultados obtenidos en el primer paso, se determinan de forma clara y concisa los objetivos de seguridad del entorno de evaluación.

- Requerimientos de seguridad de TI

Definen a detalle los requerimientos de seguridad de las TI que tendrán que ser cubiertos por el objeto de evaluación o por el entorno.

Para ello debe considerarse:

- ✓ Una valoración de los bienes que permita determinar el nivel de seguridad y de garantía que serán necesarios.

- ✓ Selección de las TI empleadas, considerando el valor de los activos que se desean protege.

- ✓ Identificación de los riesgos a los que están expuestos los activos de la organización.

- ✓ Consideración de la factibilidad técnica, los costos y los tiempos disponibles.

- Justificación

En esta etapa se justifica el trabajo desarrollado, considerando dos aspectos fundamentales, los objetivos y requerimientos de seguridad, (véase figura 2.8).

- ✓ *Justificación de los objetivos de seguridad:* tiene como meta demostrar que el conjunto de los objetivos de seguridad y el entorno definido son fáciles de seguir y que es conveniente cubrirlos

- ✓ *Justificación de los requerimientos de seguridad*: demostrará la gran utilidad que implica reunir el conjunto de requerimientos de seguridad y lo que debe seguirse para alcanzar los objetivos planeados.

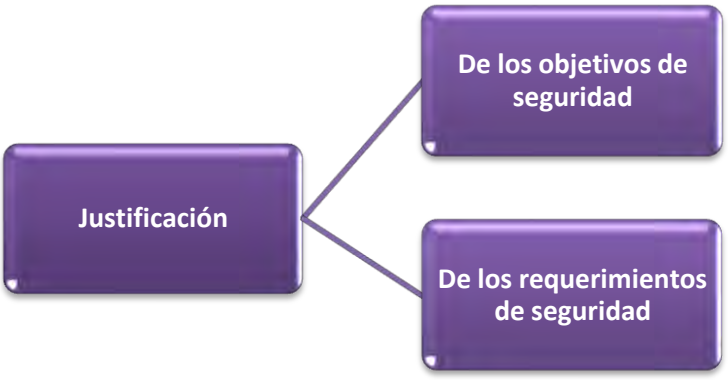

Figura 2. 8 Aspectos fundamentales de la justificación.

La metodología relacionada con los PP descrita anteriormente corresponde a la teoría de forma general cuya aplicación particular, la cual se muestra a continuación, está enfocada en la problemática existente con la manipulación de la información confidencial gestionada y almacenada por las compañías aseguradoras, lo cual permite abrir el panorama de estudio y será el punto de partida para la creación posterior de buenas prácticas.

c) Caso práctico: Perfil de protección de las compañías aseguradoras

El modelo de perfil de protección utilizado para explicar los requerimientos de seguridad, en las compañías aseguradoras es un caso particular donde se ejemplifica el uso de la metodología de los perfiles de protección, está basado en la estructura que previamente fue explicada y representada por la figura 2.4, presentando cada una de las etapas, desde el planteamiento, que permitirá la comprensión de la problemática, hasta el estudio de diversas alternativas que colaboren con la búsqueda de una solución óptima y satisfactoria, para la organización.

- Introducción:

Las compañías aseguradoras manipulan y recaudan información confidencial, donde ésta contendrá los datos personales de los clientes y todo tipo de información que requiera algún consentimiento explícito para poder ser utilizada o difundida, considerando que la *Ley de Transparencia y Acceso a la Información Pública Gubernamental (IFAI)*, en su *artículo 18* define como *información confidencial a aquellos datos personales que requieran algún tipo de consentimiento para poder ser difundidos, distribuidos o comercializados en los términos establecidos por la misma información*. De esta forma se debe establecer la importancia de crear medidas de seguridad para dicha información, ya que al ser distribuida o manipulada de forma inadecuada, se atenta contra la seguridad física, la privacidad y la intimidad de los propietarios de esos datos y a su vez de la confiabilidad en el servicio proporcionado por la compañía aseguradora.

Además de ello en México no se tiene, a diferencia de otros países como Japón, Estados Unidos y Canadá, una Ley que proteja este tipo de información de ataques a la que pueda ser sujeta, México cuenta con una serie de propuestas para la reforma de artículos a la *Constitución Política de los Estados Unidos Mexicanos*, en sus *artículos 6 y 16* además de que se cuenta en el estado de Colima con una Ley Estatal, que podría ser la base para crear en un futuro una Ley Federal que contemple el tema de la protección de los datos personales y a su vez se consideren los ataques de tipo informático que se podrían sufrir en caso de ser información electrónica la que se manipule.

La forma en la cual es manipulada la información confidencial que emplean las aseguradoras se describe brevemente, con el objeto de comprender las etapas por las cuales pasa la información de una forma física hasta una electrónica y el papel sobresaliente que tiene la criptografía para la protección de la información.

Proceso del manejo de la información en las compañías aseguradoras:

- ✓ Los **agentes**, quienes son empleados de la compañía, recaudan la información confidencial de los clientes mediante documentos físicos.

- ✓ Estos documentos son llevados, al lugar donde se encuentran los **capturistas**, para que ellos procedan a la transformación a medios

electrónicos de la información física recibida. Otra de las funciones que desempeñarán será el cifrado de la información (ya en forma electrónica), mediante el uso de la criptografía asimétrica y con la clave pública del **custodio**, definido como aquella persona que posee una clave privada, (únicamente conocida por él), lo cual lo convertirá en la única persona que pueda poner en claro dicha información.

- ✓ La información ya cifrada se almacenará en un acervo digital cifrado, el cual estará controlado bajo un *Sistema de Identificación Anonimizado*, con el objeto de que la información contenida en dicho acervo pueda pertenecer a clientes que provengan de distintas compañías de seguros.

- ✓ Por último, la distribución de la información confidencial, a terceros estará bajo la responsabilidad del **custodio**, quien para realizar dicha entrega deberá de documentarla y sólo estará facultado para dicha acción bajo instrucciones especificadas por escrito.

Una vez descrito el proceso por el cual la información es manipulada, es importante hacer mención que el objetivo principal de este trabajo, es el planteamiento de buenas prácticas, que permitan una disminución de las vulnerabilidades, que puedan estar presentes en cada una de las etapas anteriormente citadas (recaudación de la información por el agente, transformación de la información a medios electrónicos por los capturistas, cifrado de la información y protección de la misma por el custodio y el Sistema de Identificación Anonimizado) y con ello evitar ataques que atenten contra los servicios de seguridad de la información (descritos en el capítulo 1), donde estos servicios son:

- ✓ Confidencialidad.
- ✓ Autenticación.
- ✓ Integridad.
- ✓ No Repudio.
- ✓ Control de Acceso.

- ✓ Disponibilidad.

- Descripción del objeto de evaluación:

Mediante esta etapa del perfil de protección se describirá el objeto de evaluación, así como también lo que se encuentra comprendido dentro y fuera de él.

Definiéndose el objeto de evaluación, como *la protección de la información confidencial utilizada por las compañías aseguradoras* y ya habiéndose mencionado anteriormente, la importancia de la creación de buenas prácticas que permitan mejorar la seguridad en la información, se identificarán entonces, los objetos que tienen un contacto directo con dicha información confidencial como son, en primera instancia, **el agente** que es aquella persona que se encargará de recolectar dichos datos de los clientes mediante documentos determinados, los cuales son otorgados por la compañía, otro de los personajes involucrados directamente con la información son **los capturistas** y ellos representan un papel muy importante puesto que se encargan de la aplicación del algoritmo criptográfico, el cual es necesario para resguardar la información electrónica, por último el personaje con mayor importancia es **el custodio**, pues éste tendrá una clave privada que le dará facultades de poner en claro la información y este personaje, tendrá una gran responsabilidad pues será el encargado de salvaguardar la información confidencial.

Una vez definidos los personajes que están en contacto directo, se procederá a describir aquellos que están en contacto con la información, pero no de forma directa, tales como el entorno en el cual la información es resguardada mientras los capturistas hacen su trabajo, o los medios empleados para el transporte de la información, desde que ésta se encuentra en manos de los agentes hasta que llega a los capturistas, otro punto importante son las condiciones físicas en las cuales se manipula la información, como escritorios y el ambiente de trabajo, además consideraciones tales como, si después de ser capturada ésta es destruida o archivada, si es el caso de que sea destruida qué métodos son empleados para hacerlo, además de los medios utilizados para almacenar la información una vez que ha sido cifrada.

- Entorno de seguridad del objeto de evaluación:

Una vez identificado el proceso por el cual la información tiene que pasar para ser protegida y ya reconociéndose los actores que intervienen en dicho proceso. Se definen las amenazas a las cuales podría estar expuesto el objeto de evaluación, las cuales podrían ser con base en el tipo de amenazas existentes:

- ✓ *Humanas:* Que podrían deberse a consecuencias por la falta de precaución en su manipulación por parte de los actores, ya sea los agentes, capturistas o el mismo custodio, también podría considerarse el robo de la información debido a mecanismos mal implementados.

- ✓ *Errores de hardware:* La cual está involucrada con aspectos como problemas en los equipos que procesan la información ya de forma electrónica, por ejemplo las computadoras, problemas con los discos duros, que ocasionarían pérdida de la información.

- ✓ *Errores de la red:* Está relacionada con los problemas en el intercambio de información y ejemplo de este tipo de amenaza podría estar presente cuando se desee intercambiar información entre sucursales, mediante el uso de Internet, o dentro de la misma organización, mediante una red local.

- ✓ *Problemas de tipo lógico:* El exponer la información confidencial, a algún tipo de código malicioso que trate de obtenerla antes de que ésta pase por el método de cifrado o códigos que intenten acceder al sistema para causar algún tipo de conflicto en las bases que almacenan la información o alteren el correcto funcionamiento del mismo.

- ✓ *Desastres:* Dentro de las buenas prácticas, se debe considerar este punto de amenaza tan importante y que pocas veces puede ser previsto, por lo cual debe estudiarse la problemática del área, tales como posibles inundaciones o medidas contra la pérdida de la información, por algún desastre ya sea de tipo natural o accidental que podría afectar la disponibilidad de la información.

- Objetivo de seguridad:

El objeto de proteger la información confidencial es para evitar, que los datos personales de los clientes de la compañía puedan ser distribuidos o manipulados por personas no autorizadas para ello, por eso es necesario realizar un estudio detallado de cada una de las etapas por las cuales la información confidencial es manipulada y a su vez, las vulnerabilidades a las cuales pueda estar expuesta.

- Requerimientos de seguridad TI:

Dentro de los requerimientos para la seguridad de la información de datos confidenciales, está como primer punto el planteamiento de un conjunto de buenas prácticas, las cuales contemplen todas aquellas medidas preventivas para la buena manipulación de la información cuyo objetivo será disminuir la posibilidad de que las vulnerabilidades sean explotadas y con ello evitar ataques que dañen la información.

- Justificación:

La creación de buenas prácticas está justificada, en la necesidad de la creación de un conjunto de recomendaciones que sean distribuidas a todos los actores involucrados en la manipulación de la información confidencial, esto con el objeto de crear conciencia en ellos y con esto disminuir los riesgos a los cuales la información esté expuesta.

La *figura 2.9* ilustra la metodología de Perfil de protección aplicado a las compañías aseguradoras.

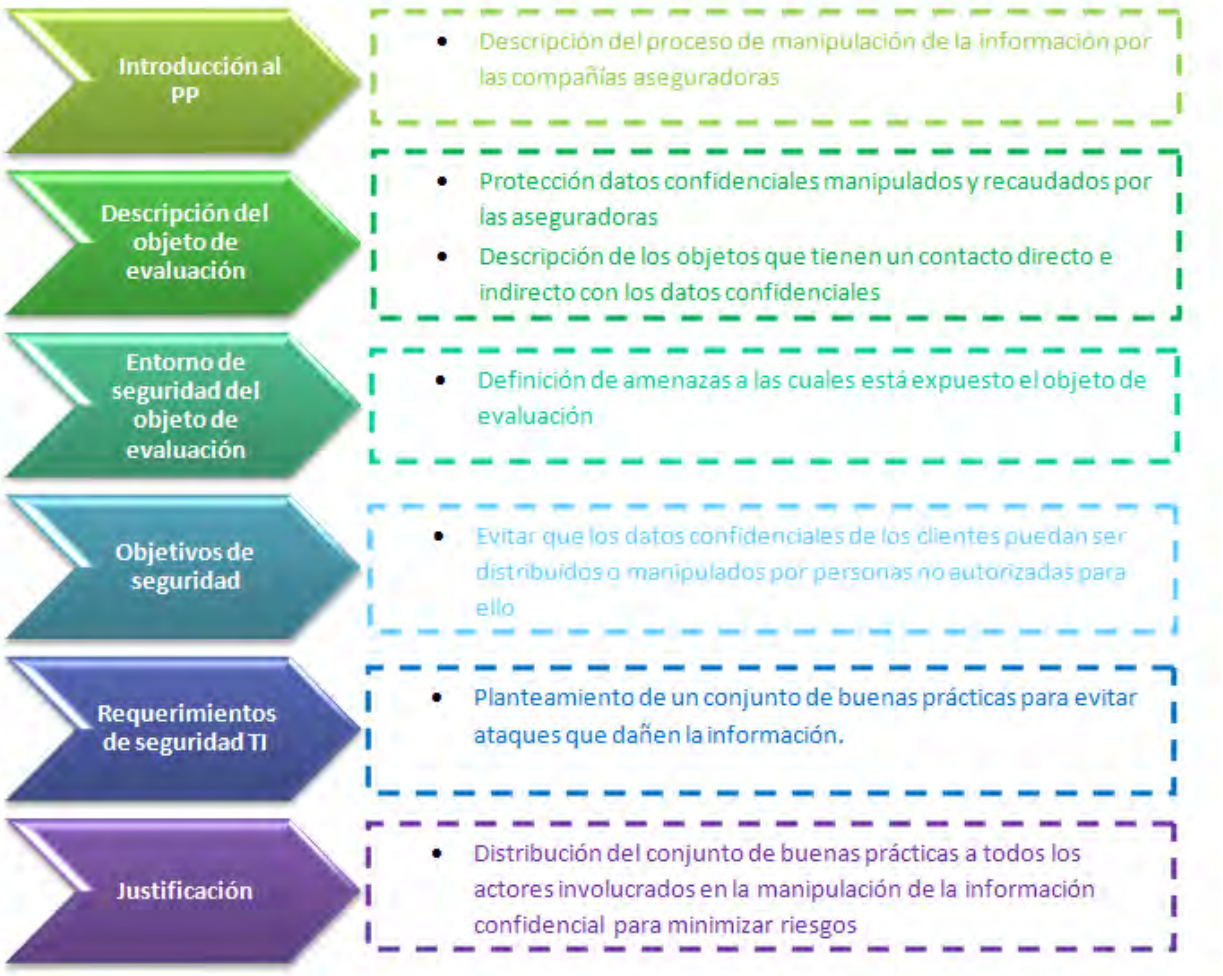

Figura 2. 9 Metodología de Perfil de protección aplicado a las aseguradoras

CAPÍTULO 3

Estándares y leyes para la protección de la información confidencial

"Lo bueno de los estándares es que hay muchos entre los que elegir"
TANENBAUM, Andrew S.

3.1 Estándares

Los organismos de estandarización se encargan de crear conjuntos de normas, estándares o reglas para lograr la aceptación de algo determinado.

De esta forma un estándar internacional relacionado con la seguridad informática surge como una medida para homogenizar las implementaciones de seguridad en diferentes organizaciones.

a) Definición

Un *estándar* (en el ámbito de la seguridad informática) es un patrón o norma aceptada y utilizada ampliamente por un gran número de interesados, con el objeto de planear, diseñar y construir productos que permitan brindar servicios que cumplan con los objetivos de seguridad requeridos.

b) Estándar ISO/IEC 17799

- Historia

El estándar *ISO/IEC 17799* es una norma internacional que proporciona una base común y recomendaciones para el desarrollo de normas de seguridad en las organizaciones –independiente del giro- con el objeto de preservar la confidencialidad, la integridad y la disponibilidad de la información.

A continuación en la tabla 3.1 se muestran los antecedentes que dieron origen al estándar ISO/IEC 17799.

Tabla 3. 1 Antecedentes del estándar ISO/IEC 17799

Fecha	Antecedente
1989	En este año surge un código de prácticas para los usuarios el cual fue creado por el Centro de Seguridad de Informática Comercial del Reino Unido dependiente del Departamento del Comercio Industrial, cuyos objetivos eran establecer un criterio de evaluación internacional y ayudar a los usuarios mediante un código de prácticas.

1993	El código de prácticas creado en 1989 fue mejorado por el NCC (Centro Nacional de Computación) y un consorcio de usuarios en representación de la industria británica, con el objetivo de hacerlo comprensible y práctico, dando origen al *PD0003* llamado *"Código de prácticas para la gestión de la Seguridad de la información"*.
1995	El British Standard Institute (BSI) publica el *BS7799*, el cual es un código de buenas prácticas para la gestión de la seguridad de la información el cual tuvo una gran aceptación por las organizaciones.
1998	El BSI publica una norma relacionada con el código de buenas prácticas ya creado en 1995, denominándolo *BS7799 parte dos*, cuyo contenido permite implementar un *SGSI (Sistema de Gestión de la Seguridad de la Información)* con base en el *ciclo Deming*[1], también conocido como *ciclo PDCA (Plan Do Check Act)*.
Octubre de 1999	Surge la propuesta del BS7799 parte uno como norma ISO[2], ya que es una norma que puede ser aplicada mundial e invariablemente en diversas organizaciones sin importar su tamaño (pequeñas, medianas o multinacionales) o el giro de éstas.
Diciembre de 2000	Previamente se realizan modificaciones y siguiendo la vía de aprobación rápida se publica el *ISO/IEC17799:2000* convirtiéndose en la nueva norma de referencia, teniendo las siguientes características: ✓ Incluye un conjunto completo de controles que conforman las buenas prácticas de la seguridad de la información. ✓ Aplicable a toda organización independiente del tamaño de ésta. ✓ Flexible e independiente de cualquier solución de seguridad concreta. ✓ Posee recomendaciones neutrales con respecto a la tecnología.
2005	En este año se hacen revisiones y actualizaciones al *ISO 17799:2000* dando lugar al *ISO 17799:2005* el cual en la actualidad forma parte de la serie 27000 dentro del *ISO 27002*.

[1] **Ciclo Deming o ciclo PDCA (Plan Do Check Act):** *(Planificar, Hacer, Verificar, Actuar) es* una estrategia de mejora continua de la calidad en cuatro pasos, basada en un concepto ideado por Walter A. Shewhart. También se denomina espiral de mejora continua. Es muy utilizado por los SGSI.

[2] **ISO** International Organization for Standardization: (Organización Internacional para la Estandarización).

El *ISO/IEC 17799* considera la información como un activo o recurso que requiere protección sin importar la forma en la cual se presente o se transmita, ya sea escrita, transmisión vía electrónica, digital, hablada etcétera. De ahí que la importancia de la seguridad de la información radique en la protección de la información de una forma oportuna y conveniente de aquellas vulnerabilidades existentes que representen un riesgo para los activos. Una vez logrado esto se asegura la continuidad de las actividades de la organización, se minimizan los daños, logrando con ello maximizar las ganancias y las oportunidades de inversión del negocio.

- Estructura

El estándar ISO/IEC 17799 está integrado por diez secciones de seguridad, derivando de ellas, los *objetivos de control* que hacen referencia a los resultados que se desean alcanzar cuando se implementan los *controles* (son prácticas, procedimientos o mecanismos que reducen el nivel de riesgo).
Las secciones de seguridad del estándar ISO/IEC 17799 se muestran en la figura 3.1

Figura 3. 1 Secciones de seguridad del estándar ISO/IEC 17799.

✓ *Política de seguridad:* proporciona a la dirección o administración ayuda para mantener la seguridad de la información en la organización, esto lo realiza mediante políticas de seguridad que son un conjunto de leyes, reglas y prácticas que regulan la forma de dirigir, proteger y distribuir los activos en una organización.

El documento que contiene las políticas de seguridad debe ser redactado de forma clara, empleando un lenguaje natural y evitando ambigüedades y en ellas deben explicarse tres aspectos principales, las *metas de seguridad de la organización*, *las propiedades de seguridad que se pretende cubrir con la aplicación de las políticas* y la forma en la cual se propone sean *implementadas dentro de la organización*.

Para lograr la implementación y reforzar el contenido de las políticas se emplean estándares, principios y procedimientos, además éstas deben ser aprobadas por la dirección o administración para su publicación y difusión entre los lugares y miembros de la organización, los cuales deben comprometerse en seguirlas para cumplir con los objetivos de seguridad planteados.

Las políticas de seguridad deben tener un propietario quien es el responsable de darles mantenimientos y revisión periódica con el objeto de considerar las nuevas tecnologías y con ello las nuevas vulnerabilidades y amenazas existentes.

✓ *Seguridad de la organización:* se encarga de manejar la seguridad de la información, de los recursos y de todo aquello que sea considerado como activo en la organización, además considera la protección de la información cuando ésta sea procesada por una organización externa.

Para llevar a cabo los objetivos de esta etapa se debe considerar lo siguiente:

- Es indispensable contar con un foro para el manejo de la seguridad de la información quien estará encargado de discutirla y analizarla en toda la organización.

- Considerar la creación de una coordinación del sistema de seguridad de la información, la cual será el punto central de contacto para abordar, tratar y tomar decisiones relacionadas con problemas de seguridad.

- Se deben definir claramente las responsabilidades para la protección de los activos que permitan realizar procesos específicos de seguridad.

- Se deben elaborar procesos de autorización que permitan asegurar la evaluación de las consideraciones de seguridad, estos procesos serán empleados para obtener la aprobación para los sistemas de procesamiento de la información que son nuevos o que han sido modificados.

- Se debe contar con un grupo de especialistas en la seguridad de la información los cuales se encargarán de proveer consejos en aspectos relacionados con la seguridad de la información usando sus conocimientos y su propia experiencia, los especialistas deben ser consultados de manera oportuna después de la ocurrencia de algún incidente de seguridad o al ser identificada alguna vulnerabilidad.

- Se debe contar con una cooperación administrativa la cual será encargada de las relaciones con los socios que comparten información y las autoridades locales que aplican las leyes, es recomendable que se cuente con una membresía en grupos de seguridad y en foros de la industria.

- Efectuar análisis independientes, los cuales serán mecanismos para analizar de manera local qué tan efectiva es la seguridad, esta revisión puede llevarse a cabo por un área interna de la organización, un administrador independiente o por una tercera organización especializada en revisiones de este tipo.

- Se deben considerar mecanismos para controlar la interacción de la tercera entidad dentro de la organización, con ello se pretende mantener la seguridad de los medios que procesan la información y a su vez de los activos a los cuales la tercera entidad tiene acceso.

- Se deben establecer medidas para el outsourcing[3], que deben estar claramente establecidas en el contrato en el cual se considerarán temas como los riesgos, los controles de seguridad y los procedimientos para los sistemas de la información.

✓ *Clasificación y control de activos*: En esta etapa se identifican los activos más importantes de la organización y una vez identificados se les asigna un dueño quien será el responsable de la protección del mismo, utilizando controles adecuados para lograrlo. Es recomendable que la responsabilidad del activo siempre quede a cargo del dueño del mismo quien deberá verificar que los activos reciban un nivel adecuado de protección.

Dentro de las acciones que pueden considerarse en esta etapa:

- Crear un inventario de activos y fijar responsables para cada uno de ellos, esto ayudará para asegurar la protección de los mismos, además permite fijar niveles de protección cuyo objetivo sea la identificación de los activos que requieran una mayor protección o que su revelación causaría daños considerables en la organización.

- Clasificar los recursos considerando la importancia para la organización, esta clasificación permitirá definir cómo se dirige, quién y cómo será protegido.

- Definir una serie de procedimientos para etiquetar y manejar la información considerando el esquema de clasificación empleado por la organización, se debe considerar que los activos se presentan tanto de forma física como electrónica.

✓ *Seguridad del personal:* considera aspectos relacionados con la contratación del personal, lo cual debe estar incluido en los contratos y ser supervisado su cumplimiento de forma periódica. Es necesario considerar la firma de un acuerdo de confidencialidad para aquellos empleados y terceras entidades que hagan uso de la información o de los sistemas que la manipulan con el objeto de evitar que personas no autorizadas tengan

[3] **Outsourcing:** proceso económico en el cual una empresa determinada mueve o destina los recursos orientados a cumplir ciertas tareas, a una empresa externa, por medio de un contrato.

acceso a ella y que su divulgación pueda representar un riesgo para la organización.

Además mediante esta etapa se evalúa la capacidad de respuesta de la organización para mitigar el riesgo generado por las interacciones humanas cuando se manipula la información.

Dentro de los objetivos de esta área está la disminución del riesgo de error, el fraude, el robo o el mal uso, además asegurar que los responsables y colaboradores en las diversas actividades de la organización estén conscientes de la importancia de la seguridad de la información, para ello se puede impartir capacitación para el personal de forma periódica, así como también la reducción de los incidentes que permitan un aprendizaje aplicado para reforzar las medidas de seguridad implementadas en la organización, para incrementar su eficiencia y efectividad.

- ✓ *Seguridad física y ambiental:* en relación a esta etapa se tiene que considerar el resguardo de todos aquellos activos que sean considerados de gran importancia para la organización, esto se debe hacer mediante el resguardo de los mismos en áreas seguras que tengan implementados controles adecuados para brindar protección ante cualquier daño, interferencia o acceso no autorizado. Es recomendable que los lugares físicos, en los cuales sea almacenada o manipulada la información, cuenten con medidas de higiene. Los objetivos principales de la seguridad personal radica en evitar que el personal no autorizado, pueda modificar, dañar o robar la información, además debe prevenir la pérdida o daño en los activos que sean vitales para continuar el flujo normal de las actividades en la organización. Para cumplir con dichos objetivos se pueden considerar las siguientes recomendaciones:

  - Para implementar la protección física se pueden crear barreras físicas que se encarguen de salvaguardar las instalaciones y los medios encargados del procesamiento de la información.

  - Considerar la implementación de controles de acceso dependiendo el área objetivo que requiera protección.

- Ubicación adecuada de los equipos para garantizar la integridad y disponibilidad física y ambiental de la información.

- Controlar la entrada y salida de los activos en la organización.

✓ *Gestión de comunicaciones y operaciones:* está relacionada con la capacidad de una organización para asegurar que las operaciones que se realizan con sus recursos sean efectuadas de forma segura y correcta.

Dentro de los objetivos de esta etapa destacan la disminución de los riesgos generados por las fallas en los sistemas, la protección de la integridad del software y de la información, asegurar y salvaguardar la información que es transmitida mediante las redes y toda la infraestructura que se emplea para ello, prevención de posibles interrupciones de las actividades económicas o daño a los activos, establecer responsabilidades y procedimientos para las operaciones de todas las instalaciones de procesamiento de información.

Para cumplir los objetivos citados con anterioridad se realizan las siguientes actividades:

- Creación de procedimientos los cuales deben estar identificados por las políticas de seguridad y los estándares de la organización, éstos deben documentarse y mantenerse y ser tratados como documentos formales y cualquier modificación debe ser autorizada por la dirección.

- Se deben controlar los cambios a las instalaciones y a los sistemas que procesan la información, cuando no se tiene control sobre éstos se desencadenarán fallas en los sistemas creando brechas de seguridad.

- Se recomienda usar el método de segregación de deberes, el cual tiene por objetivo reducir el riesgo del mal uso, accidental o deliberado del sistema, este método consiste en la separación y rotación de obligaciones.

- Creación de mecanismos encargados de la supervisión y proyección de las capacidades de la organización para evitar la interrupción de la disponibilidad, dichas proyecciones deben considerar los nuevos

requerimientos de activos y sistemas, considerando las tendencias actuales para ser proyectadas en la información procesada por la organización.

- Evaluación de los cambios de los sistemas que permitan asegurar la continuidad en la confidencialidad, disponibilidad e integridad.

- Implementar controles para disminuir el riesgo por la introducción de código malicioso, es importante considerar que los usuarios sean notificados de los peligros existentes cuando hacen uso de software no autorizado o malicioso, a su vez los encargados deben introducir medidas para detectar, prevenir o impedir el uso de éste.

- Control para el manejo de las operaciones de forma segura en la infraestructura de la red, también se deben considerar los controles requeridos para protección de la información en los medios de almacenamiento con el objetivo de evitar la pérdida, robo, alteración de la información resguardada en ellos.

- Implementar controles para los procesos de intercambio de información, en los cuales deben considerarse los acuerdos con el usuario final y los mecanismos de transporte de la información que es intercambiada entre las organizaciones. Para ello es necesario establecer procedimientos y estándares que protejan la información y los medios empleados para el intercambio.

✓ *Control de acceso:* esta sección considera la capacidad con la que cuenta la organización para controlar el acceso a los recursos y activos de la organización. Dentro de los principales objetivos destacan prevenir accesos no autorizados, protección de los servicios de red, detección de actividades no autorizadas, asignación de contraseñas y definición de privilegios. Para cumplir con los objetivos mencionados es necesario considerar los requerimientos de seguridad de la organización.

✓ *Desarrollo y mantenimiento de sistemas*: se encarga de evaluar la capacidad de la organización para asegurar que los controles de seguridad definidos para el sistema de información sean incorporados y se les proporcione

mantenimiento. Los objetivos de esta etapa consisten en asegurar la construcción de sistemas operacionales, la prevención de la pérdida, modificación o mal uso de la información, también asegura que los proyectos y las actividades sean aplicadas adecuadamente, además se encarga de mantener la seguridad del software del sistema y de los datos que son gestionados por la aplicación.

La criptografía tiene un papel importante dentro de esta etapa debido a que permite mantener la confidencialidad, autenticidad y la integridad de la información, la aplicación de métodos criptográficos permite proteger la información que se considera tiene un grado de importancia elevado para la organización y que su divulgación o pérdida podría ocasionar graves consecuencias.

Otro punto de gran importancia está relacionado con la seguridad en las aplicaciones desarrolladas evitando con ello que la información manipulada por dichos sistemas esté expuesta a cualquier tipo de amenaza.

- ✓ *Plan de continuidad del negocio:* esta etapa tiene como objetivo evitar la interrupción en las actividades y procesos críticos de la organización además de evaluar el impacto de los incidentes en la disponibilidad de los activos y en la continuidad de los procesos realizados con ellos.

  Para lograr estos objetivos deben considerarse las siguientes actividades:

  - Implementación de procesos de administración de la continuidad en las actividades realizadas dentro de la organización con el objeto de reducir la interrupción como consecuencia de fallas de seguridad, desastres o cualquier tipo de incidente que ponga en riesgo la disponibilidad. Se deben considerar las consecuencias que podrían ocasionar dichos incidentes, para ello es necesario la creación de **planes de contingencia preventivos y correctivos**, cuya finalidad será tanto evitar los incidentes que pudieran presentarse así como también asegurar la restauración oportuna de las operaciones en el menor tiempo posible.

  - Es necesario realizar pruebas de continuidad de forma periódica para asegurar que éstos sean actualizados y eficientes además se requiere

proporcionar un mantenimiento que permita asegurar la eficiencia, garantizando con ello la continuidad en las actividades realizadas por la organización.

- ✓ *Cumplimiento:* en esta sección se considera la capacidad con la que cuenta la organización para permanecer en conformidad con los requerimientos reguladores, disposiciones legales y de seguridad. Los objetivos de esta etapa son, evitar cualquier ambigüedad que pueda presentarse en relación con las cuestiones legales que deban ser consideradas para cualquier requisito de seguridad, es necesario que siempre estén claramente especificados y fundamentados los términos legales, además se debe asegurar la conformidad entre los sistemas de seguridad con las políticas o estándares de la organización, otro aspecto considerado es la reducción de la interferencia externa a los sistemas y los procesos gestionados por éstos, lo que incrementará la eficiencia de la organización.

  Para cumplir con los objetivos esta etapa contempla las siguientes actividades:

  - Los requerimientos legales requieren de conocimientos sobre legislaciones, derechos de propiedad intelectual, privacidad de datos, prevención de abuso, recopilación de evidencias y regulación de criptografía.

  - Por otro lado los requerimiento técnicos son una serie de mecanismos encargados de verificar la ejecución e implementación de las políticas de seguridad, para ello deben realizarse revisiones periódicas las cuales siempre se llevarán a cabo en comparación con las políticas apropiadas de seguridad y las plataformas técnicas.

  - Es necesario además realizar revisiones en los sistemas que permitirán maximizar la eficiencia y minimizar con ello la desorganización, logrando con ello la preservación de la confidencialidad, disponibilidad e integridad en los activos y sistemas de la organización.

- Beneficios

La seguridad de la información es un asunto de cambios que considera los requerimientos de la organización y la conservación de los servicios de confidencialidad, integridad y disponibilidad.

El proceso de la seguridad informática se basa en principios y mejores prácticas con la finalidad de prevenir, detectar y brindar una solución a las brechas o fracturas de seguridad existentes, de tal forma que puedan repararse los daños o pérdidas que se hayan presentado como resultado y que pongan en riesgo la seguridad de la información.

Los beneficios del estándar ISO/IEC 17799 son:

- ✓ Ofrece un punto de referencia para construir la seguridad de la información en la organización, además cuenta con mecanismos para lograr la implementación de los procesos en ésta.
- ✓ Proporciona a la organización una metodología estructurada y reconocida internacionalmente.
- ✓ Define un conjunto de procesos para evaluar, implementar, mantener y manejar la seguridad de la información.
- ✓ Permite a la organización la creación de políticas, estándares, procedimientos y principios.
- ✓ La certificación permite a las organizaciones demostrar su propio estado de seguridad de la información y con ello evaluar el de las organizaciones asociadas.
- ✓ El contar con una certificación permite a la organización tener una ventaja frente a los competidores no certificados.
- ✓ Una certificación proporciona a una organización una mayor seguridad como empresa, una planeación y gestión de la seguridad más efectiva, le permite alianzas comerciales, abrirse camino de forma más confiable en el

comercio electrónico, una mayor confianza de sus clientes, auditorias de seguridad más precisas y confiables y disminuye su responsabilidad civil.

Con las nuevas actualizaciones al *ISO/IEC 17799* y su incorporación a la serie 27000 se cuenta con once secciones adicionando una a las anteriormente citadas, la cual está relacionada con la *gestión de incidentes de seguridad de la información* que tiene como actividades principales, notificar a las organizaciones cuáles son considerados como sus puntos débiles y los eventos que se han presentado y representen un peligro para la información y los activos identificados, además de ello considera la elaboración de una recopilación con los incidentes de seguridad detectados y las mejoras para su corrección y prevención.

c) Estándares serie 27000

Mediante la familia de normas de la *serie ISO 27000*, las organizaciones aseguran ante grupos de su interés tales como: socios, clientes, proveedores y trabajadores, que se han implementado medidas que garantizan la gestión adecuada de la seguridad de la información que manipulan. Los rangos de numeración que ha reservado ISO van de *27000* a *27019* y de *27030* a *27044*.

En tabla 3.2 se muestra una descripción de cada uno de los estándares que integran la serie 27000:

Tabla 3. 2 Estándares de la serie 27000

Estándar	Descripción
ISO 27000	Contiene los términos y definiciones empleados en toda la serie 27000, ya que la aplicación de cualquier estándar requiere que el vocabulario esté claramente definido para evitar errores o ambigüedades.
ISO 27001	Fue publicada el 15 de octubre del 2005, teniendo como antecedente la segunda parte del estándar BS7799. Esta norma es fundamental en la serie ya que contiene los requisitos requeridos para la implantación del *Sistema de Gestión de Seguridad de la Información (SGSI)*, considerando en su anexo A resúmenes de los objetivos de control y los controles que desarrolla la ISO 27002:2005 para que las organizaciones puedan seleccionarlos y lograr el desarrollo de sus SGSI.

ISO 27002	Publicada desde el 1 de julio de 2007. Esta norma es una guía de buenas prácticas que describe los objetivos de control y los controles recomendados para mantener e incrementar los niveles de seguridad de la información en la organización. Los lineamientos establecidos dentro de este estándar corresponden al ISO/IEC 17799. No es certificable.
ISO 27003	Es una guía de implementación de un *SGSI* e información relacionada con el modelo *PDCA* y los requerimientos de sus diferentes fases.
ISO 27004	Específica las métricas y las técnicas aplicables para determinar la eficiencia de un SGSI y de los controles relacionados.
ISO 27005	Consiste en una guía de técnicas para la gestión del riesgo de la seguridad de la información. Esta norma servirá de apoyo a la ISO 27001 y a la implantación de un SGSI.
ISO 27006	Esta norma establece los requisitos para la acreditación de las entidades de auditoría y certificación de los Sistemas de Gestión de Seguridad de la Información.
ISO 27007	Consiste en una guía de auditoría de un SGSI.
ISO 27011	Proporciona una guía de gestión de seguridad de la información específica para el área de las telecomunicaciones.
ISO 27031	Esta norma contiene una guía de continuidad del negocio en relación con las tecnologías de la información y de las comunicaciones.
ISO 27032	Proporciona una guía relacionada con la ciberseguridad.
ISO 27033	Esta norma está integrada en siete partes: ✓ Gestión de seguridad de redes. ✓ Arquitectura de seguridad de redes. ✓ Escenarios de redes de referencia. ✓ Aseguramiento de las comunicaciones entre redes mediante gateways.

	✓ Acceso remoto. ✓ Aseguramiento de comunicaciones en redes mediante *VPNs*[4]. ✓ Diseño e implementación de seguridad en redes.
ISO 27034	Esta norma es una guía de seguridad en aplicaciones.
ISO 27799	Este estándar permite la gestión de seguridad de la información en el sector.

3.2 Leyes y organismos en México.

Como consecuencia de la aparición y desarrollo de las tecnologías de la información (TI), *(las cuales permiten la transmisión y almacenamiento de información en grandes bases de datos)* ha surgido con mayor auge la protección de los datos personales, lo que actualmente para las organizaciones se ha convertido en un tema fundamental.

La razón para brindar protección a los datos personales radica en que éstos proporcionan información relativa a los individuos que lo identifican o permiten su identificación, permitiéndoles a éstos una interacción con una o más organizaciones sin que pueda presentarse confusión alguna, además de ello permiten la obtención de bienes y servicios, tal es el caso de las compañías aseguradoras quienes a cambio de este tipo de información y el pago de sus servicios proporcionan un respaldo a sus clientes.

El tipo de información considerada como *datos personales son: el origen, la edad, el lugar de residencia o cualquier tipo de trayectoria, ya sea académica, laboral o profesional*. En el caso de las compañías aseguradoras el tipo de datos personales está clasificado como sensible ya que éstos detallan aspectos delicados tales como el estado de salud ya sea físico o mental, las características físicas, la vida sexual y demás información de los clientes que resulta altamente confidencial.

Cabe señalar la importancia del proceso de ***clasificación de la información***, el cual contribuirá para que la organización pueda separar y diferenciar todos aquellos datos que sean de libre acceso de los que son restringidos y que a su vez permita establecer diferentes medidas de seguridad considerando la clasificación establecida, ésta debe ser

[4] **VPN (Virtual Private Network):** *(Red Privada Virtual)* es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet.

rigurosa pero a la vez eficiente, de tal forma que no se convierta en un proceso impracticable y costoso.

Considerando lo establecido en el *Capítulo III Información reservada y confidencial* de la *Ley Federal de Acceso a la Información Pública Gubernamental*, la información puede ser clasificada de dos formas:

- ✓ *Información reservada:* es aquella cuya difusión comprometa la seguridad nacional, la seguridad pública o la defensa nacional, que disminuya las negociaciones o relaciones internacionales, esto incluye la información que otros estados u organismos internacionales proporcionen con carácter confidencial al Estado Mexicano, que pueda dañar la estabilidad financiera, económica y monetaria del país, causar perjuicio a las actividades de verificación del cumplimiento de las leyes, secretos comerciales, averiguaciones previas, expedientes judiciales.

  Además, esta clasificación incluye información que pone en riesgo la vida, la seguridad o la salud de cualquier persona, en esta parte se consideran *los expedientes médicos, los dictámenes* y toda aquella información relacionada con la salud que sea utilizada por las compañías aseguradoras para la evaluación de los candidatos.

- ✓ *Información confidencial:* esta clasificación incluye *los datos personales que requieran el consentimiento de los individuos para su difusión, distribución o comercialización*, tal es el caso del origen, la edad, el lugar de residencia, la trayectoria laboral o profesional, sexo, las preferencias sexuales e información que permita la identificación del individuo.

Debido a la preocupación que surge no sólo en México, sino a nivel mundial con relación a la protección de los datos personales, se han creado iniciativas que han servido de antecedentes para su propagación en el mundo, tal es el caso de la iniciativa del Consejo de Europa, el cual ha invitado a diversas autoridades de distintos países para crear un espacio de reflexión y concientización en su población, relacionado con el uso, la obtención y transmisión de la información personal.

Por todo esto, el Comité de Ministros del Consejo de Europa decidió el 26 de abril del 2006 declarar el día *28 de enero* como el *"Día de la protección de los datos personales"*,

con motivo de celebrar el aniversario de la firma del Convenio 108, mediante el cual los países firmantes se comprometen a llevar a cabo las reformas necesarias en su legislación para contemplar los siguientes apartados:

- ✓ La recolección de datos personales deberá llevarse a cabo y tratarse exclusivamente con fines legítimos.
- ✓ Los datos personales recolectados deberán conservarse no más del tiempo estrictamente necesario.
- ✓ Considerando la finalidad con la que cumplen, los datos personales recolectados deben ser verdaderos y cantidades no excesivas.
- ✓ Garantizar la confidencialidad de los datos clasificados como sensibles además de proporcionar el derecho a los propietarios de la información, el acceso o en su caso la solicitud de la corrección de los datos cuando hubiera alguna actualización o algún error.

Otros países que han considerado la protección de los datos personales son los que se encuentran en la tabla 3.3.

Tabla 3. 3 Aportaciones de algunos países para la protección de los datos personales.

País	Aportaciones
España	✓ *Ley Orgánica 15/1999*, del 13 de diciembre, de Protección de Datos de Carácter Personal (B.O.E. Núm. 298, 14/12/1999). ✓ *Real Decreto 1332/1994*, del 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, del 29 de octubre, de Regulación del Tratamiento Automatizado de Datos de Carácter Personal (B.O.E. Núm. 147, 21/6/1994). ✓ *Real Decreto 994/1999*, del 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal (B.O.E. Núm. 151, 25/6/1999). ✓ *Instrucción 1/2000*, del 1 de diciembre, de la Agencia de Protección de datos, relativa a las normas por las que se rigen los movimientos internacionales de datos.

Portugal	✓ *Lei n.º 67/98* de 26 de Outubro. Lei da protecção de dados pessoais (transpõe para a Ordem Jurídica Portuguesa a Directiva 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de outubro, relativa à protecção das pessoas singulares no que diz respeito ao tratamento dos dados pessoais e á livre circulação desses dados).
Argentina	✓ *Ley 25.326*. Ley de Protección de Datos Personales. (Publicada en el Boletín Oficial del 2/11/2000, Núm. 29517). ✓ *Decreto 995/2000.* Habeas Data. (Publicado en el Boletín Oficial del 2/11/2000, Núm. 29517 ✓ *Decreto 1558/2001*. Protección de Datos Personales (Publicado en el Boletín Oficial del 3/12/2001, Núm. 29787).
Colombia	✓ *Constitución Federal de la República (art. 15).*
Costa Rica	✓ *Proyecto de Ley de Habeas Data*. Expediente Núm. 12.827.
Chile	✓ *Ley Núm. 19.628* sobre Protección de la vida privada. ✓ *Decreto Núm. 779/2000*. Prueba el Reglamento del Registro de Bancos de Datos Personales a Cargo de Organismos Públicos.
Perú	✓ *Ley Núm. 27489*. Ley que regula las centrales privadas de información de riesgos y de protección al titular de la información (Promulgada el 27/6/2001, publicada el 28/6/2001).
Uruguay	✓ *Proyecto de Ley -* Derecho a la información y acción de habeas data.

Además de aportaciones de países como Alemania, Australia, Bélgica, Bulgaria, Canadá, Chipre, Dinamarca, Estonia, Eslovaquia, Eslovenia, Estados Unidos, Francia, Finlandia, Grecia, Holanda, Hungría, India, Irlanda, Islandia, Italia, Japón, Letonia, Lituania, Luxemburgo, Malta, Mónaco, Nicaragua, Noruega, Zelanda, Polonia, Reino Unido, República Checa, Rumania, Suecia, Suiza y Tailandia lo cual demuestra el gran interés de las naciones por la implementación de medidas de protección para la información confidencial, los datos personales, la privacidad y con ello al individuo mismo.

Debido a la importancia con relación a la protección de los datos personales, específicamente aquellos relacionados con cuestiones médicas, cabe señalar la existencia de la ***Ley de Portabilidad y Responsabilidad del Seguro Médico, HIPAA*** *por sus siglas en*

inglés (Health Insurance Portability and Accountability Act) ésta es una ley federal aprobada el 16 de Agosto de 1996 por el congreso de Estados Unidos, la cual se concentra en la protección de la confidencialidad, la disponibilidad y la integridad de los datos de los pacientes, sus objetivos principales son:

- ✓ Facilitar a las personas el mantener su seguro médico.
- ✓ Protección de la confidencialidad y seguridad de la información bajo el cuidado médico.
- ✓ Ayudar a la industria relacionada con el cuidado de la salud a controlar los costos administrativos

El *Título II* conocido como la *Simplificación Administrativa,* en uno de sus apartados establece puntos para garantizar la seguridad y la privacidad de la información médica. De esta forma todo proveedor de salud, incluyendo las compañías aseguradoras, deben considerar lo establecido por la *HIPAA* con relación a las reglas de privacidad sobre la información de los pacientes.

Dos cláusulas de *HIPPA* están relacionadas con la información médica protegida[5]:

- ✓ *Regla de privacidad:* establece medidas para que el personal médico no pueda hacer uso o revelación de la información médica protegida del paciente sin su consentimiento.

  Las protecciones provistas en la Regla de privacidad tienen tres objetivos:

  - Brindar a las personas un control mayor sobre su información médica personal.
  - Limitar lo que otros pueden hacer con la información médica protegida.
  - Salvaguardar la información médica identificable individualmente.

  El saber que la información médica personal está protegida, aumentará la confianza entre las personas y aquellos que proveen y pagan por su atención.

- ✓ *Regla de seguridad:* especifica un conjunto de procesos empresariales y requisitos técnicos que los proveedores, planes médicos y oficinas de compensación deben seguir para garantizar la seguridad de la información médica protegida.

[5] **Información médica protegida:** información que se relaciona con la salud o algún padecimiento físico o mental, pasado, presente o futuro.

Las autoridades de México, en su labor por concientizar y establecer medidas de protección de los datos personales han creado iniciativas, leyes, propuestas e instituciones que permitan modificaciones en la Constitución, las cuales deberán contemplar la necesidad de México en proteger la información que constantemente es manipulada por sistemas tecnológicos, los cuales siguen la tendencia del mercado hacia la automatización de los procesos para el consumo, se debe considerar que los datos personales clasificados como sensibles requieren un manejo adecuado y confiable por parte de las entidades que los manipulan protegiendo la integridad, la disponibilidad y la confidencialidad de los mismos y de los individuos propietarios. Es necesario que las autoridades regulen los datos personales que son transferidos y transmitidos usando las nuevas tecnologías con el objeto no sólo de lograr un avance en el crecimiento del país sino además evitar todos aquellos delitos generados por la manipulación incorrecta de esta información de la cual pueda obtenerse un lucro o beneficio económico pero que en algunos puede ser origen de crímenes y delitos que cobren vidas cuyas pérdidas por siempre será irreparables.

En la tabla 3.4 se muestran los artículos existentes, las iniciativas, las reformas y todo aquello que ha considerado el gobierno mexicano para la protección de la información, la privacidad, los datos personales y el acceso a la información.

Tabla 3. 4 Acciones del gobierno de México para la protección de los datos personales.

Iniciativa	Descripción
Artículo 6 *Constitución Política de los Estados Unidos Mexicanos*	Está relacionado con el derecho a la información, el cual será garantizado por el Estado, que para efectos de la regulación se considera como el derecho del individuo a tener acceso a su información contenida en bancos de datos los cuales no deberán ser manejados de forma indebida. Se han realizado propuestas de reformas que aún no han sido aprobadas y que representan avances significativos en materia de protección de los datos personales: Estas propuestas consideran lo siguiente: ✓ La información en posesión de autoridades, organismos estatales o municipales es pública y sólo podrá ser reservada de forma temporal por razones de interés público considerando los términos establecidos por las leyes. ✓ Los datos personales e información relacionada con la vida privada será protegida en los términos establecido por las leyes.

	✓ Toda persona sin necesidad de justificación alguna tendrá acceso gratuito a la información pública así como los titulares de los datos personales podrán acceder a éstos para realizar rectificaciones.
Artículo 16 *Constitución Política de los Estados Unidos Mexicanos*	Establece: *"Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento estricto de la autoridad competente, que funde y motive la causa legal del procedimiento"*. Las propuestas de modificación a este artículo consisten en reconocer el derecho a la protección de los datos personales como derecho fundamental, estableciendo que toda persona tendrá el derecho a la protección de sus datos personales y el acceder a éstos para realizar rectificaciones, cancelaciones o destrucción, considerando los términos establecidos por las leyes.
Artículo 73 *Constitución Política de los Estados Unidos Mexicanos*	Considera que de la misma forma en la que las instituciones gubernamentales protegen la información que poseen en sus archivos, las organizaciones particulares como los bancos, los hospitales privados, las universidades, profesionistas entre otros, puedan ser reguladas en cuanto al manejo de los datos personales o información relativa a las personas. Siendo el Congreso de la Unión quien tendrá facultad para la regulación en estas organizaciones. Esta propuesta está pendiente de aprobación pero sin duda alguna representaría un paso considerable para la incursión en la Constitución de artículos que contemplan la protección de los datos personales por entidades del sector privado.
Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental	Esta ley fue publicada en el Diario Oficial de la Federación el *11 de julio de 2002* y sus objetivos principales son: ✓ Garantizar la protección de los datos personales en posesión de los sujetos obligados. ✓ Acceso y corrección de los datos personales por los titulares de los mismos para lo cual se deben establecer las autoridades encargadas para la protección. El campo de acción de esta ley es obligatorio únicamente para los poderes públicos del Estado federal.

	Es importante hacer mención que los artículos 13 y 14, los cuales consideran que cierta información puede ser clasificada como reservada y a su vez el artículo de esta ley contempla que hay información que puede considerarse como confidencial y la cual estará definida como el conjunto de datos personales que requieran el consentimiento de los titulares para su difusión, distribución o comercialización.
Fracción I del artículo 76 BIS *Ley Federal de Protección al Consumidor*	En este apartado se establece como obligación para los proveedores de preservar la confidencialidad de la información y a su vez se les prohíbe la difusión o transmisión a otros proveedores, a menos que se cuente con la autorización del consumidor o se haya solicitado por alguna autoridad.
Código de comercio *Código Civil y de Procedimiento Civiles*	En éste se regula el llamado "*Mensaje de Datos Personales (MDP)*" que surge por la creciente de las Tecnologías de la Información (TI), el MDP es considerado en el *artículo 89* del Código de Comercio y definido como aquella información generada, enviada, recibida, archivada o comunicada a través de medios electrónicos, ópticos o cualquier otra tecnología. Por otro lado el *artículo 91* define que un sistema de información es cualquier medio tecnológico empleado para operar los mensajes de datos. En ellos se requiere tener un gran cuidado en el tratamiento de la información y comunicación, siempre considerando la protección del derecho a la privacidad de las personas.
Ley estatal de Estado de Colima *Ley de Protección de Datos del Estado de Colima*	Esta ley establece que los datos personales deberán ser obtenidos y ser sujeto de tratamiento cuando éstos sean adecuados, pertinentes y no excesivos. Los datos personales deberán ser correctos y actualizados, obtenidos por medios lícitos y se requerirá el consentimiento del propietario.
Iniciativa de Ley Federal de Protección de Datos Personales	Los objetivos de esta iniciativa son: ✓ Que el interesado pueda acceder a los datos personales que le conciernen ✓ Que toda persona pueda tener acceso a los registros, los archivos y los bancos de datos públicos o privados de carácter público y conocer su uso o fin para el que están destinados

	✓ Que el interesado pueda pedir la inclusión, actualización, complementación, rectificación, reserva, suspensión y cancelación de los datos relativos a su persona
Ley de Protección de Datos Personales para el Distrito Federal	Es una ley de carácter público, publicada el 3 de Octubre de 2008, en la Gaceta Oficial del Distrito Federal. Tiene por objeto establecer los principios, derechos, obligaciones y procedimientos para regular la protección y tratamiento de los datos personales en posesión de los entes públicos.
Ley de Instituciones de Crédito	Considera en su contenido guardar la confidencialidad sobre la información a la cual se tiene acceso durante la celebración de operaciones de los clientes salvo que se cuente con el consentimiento expreso de los mismos.
Ley Federal del Derecho de Autor *Capítulo IV De los programas de computación y bases de datos* *Artículo 109*	Manifiesta la protección de la información relacionada con las personas, que sea de carácter privado y que esté contenida en las bases de datos, expresando que para su publicación, reproducción, divulgación, comunicación pública y transmisión de dicha información será necesaria la autorización previa del propietario
Ley para regular las sociedades de información crediticia *Capítulo II De las bases de datos*	Está relacionada con la protección de la información por parte de las sociedades de información crediticia, las cuales deberán garantizar la protección de la información adoptando las medidas de seguridad y control necesarias para evitar el manejo indebido de la información *(el cual se concibe como cualquier acto u omisión que cause daño al patrimonio del sujeto del que se posee información)*
Ley General de Salud *Artículo 77 BIS* **y** **Reglamento de la Ley General de Salud en materia de prestación de servicios de atención médica** *Artículo 29 y 32*	Mencionan aspectos relacionados con el derecho a la información del que goza el beneficiario de los servicios de salud, de esta forma los beneficiarios tienen derecho a: ✓ Recibir información suficiente, clara, oportuna y veraz, así como la orientación que sea necesaria con respecto a la atención de su salud y sobre los riesgos y alternativas de los procedimientos diagnósticos, terapéuticos y quirúrgicos que se le indiquen o apliquen ✓ Todo profesional de la salud estará obligado a proporcionar al usuario y en su caso a sus familiares, tutor o representante legal, información completa sobre el diagnóstico, pronóstico y tratamiento correspondiente

	✓ Contar con su expediente clínico ✓ Los establecimientos para el intercambio de enfermos estarán obligados a conservar los expedientes clínicos de los usuarios, por un periodo mínimo de cinco años y ser tratados con confidencialidad

El contenido de la tabla 3.4 permite ver que México cuenta con grandes iniciativas en reformar la Constitución para considerar la protección de los datos personales ya que actualmente la carencia de un sustento constitucional imposibilita al Poder Legislativo en la expedición de una ley a nivel federal que regule la protección y que considere ambos sectores, el público (considerando que en este ámbito hay un gran avance por parte del IFAI[6]) y el privado, al cual pertenecen las compañías aseguradoras.

Además cabe señalar que en México no se cuenta con leyes que definan las sanciones relacionadas con delitos informáticos como tal *(considerado la protección de la información confidencial en formato electrónico)*, lo que conlleva a otorgar sanciones a estas faltas, recurriendo a la interpretación de las leyes vigentes en las cuales puedan incluirse las violaciones en las que haya incurrido el delito y de esta forma castigar a los responsables, dentro de estas leyes se encuentran las que se mencionan a continuación:

- ✓ *Correo:*
  - Código Penal
- ✓ *Propiedad:*
  - Código Penal
  - Ley de Propiedad
  - Ley Federal del Derecho de Autor
- ✓ *Delitos informáticos:*
  - Código Penal
  - Ley de Propiedad
  - Ley Federal de Derecho de Autor
  - Código Penal para el Distrito Federal
  - Código Penal del Estado de Sinaloa

[6] **IFAI (Instituto Federal de Acceso a la Información Pública)**

- Iniciativa de Ley Federal de Protección de datos personales
- Ley de Protección de datos personales del Estado de Colima

✓ *Privacidad:*

- Iniciativa de Ley Federal de Protección de datos personales
- Ley de Protección de datos personales del Estado de Colima
- Ley de Transparencia y Acceso a la Información Pública Gubernamental

✓ *Cómputo forense:*

- Código Federal de Procedimientos
- Código de Comercio

✓ *Contratos electrónicos y firma electrónica:*

- Código de Comercio
- Código Civil Federal y algunos
- Código Fiscal de la Federación
- Ley del Mercado de Valores
- Ley del Federal de Protección al consumidor
- Ley Federal del Procedimiento
- Ley de Instituciones de Crédito
- NOM[7] 151-SCFI[8]-2002

✓ *Contenidos de internet:*

- Código Penal Federal del Distrito Federal

[7] **NOM**: Norma Oficial Mexicana
[8] **SCFI:** se escriben esas siglas o las del organismo que se encarga de realizar la norma, comúnmente es SCFI

CAPÍTULO 4

La criptografía como herramienta para la protección de la información confidencial

"La seguridad de un sistema no debe depender de mantener en secreto el algoritmo, sino sólo de mantener secreta la clave."

Principio de Kerckhoffs.

4.1 La criptografía y el sistema de cifrado

a) Definición

La *criptografía* cuyo origen etimológico proviene del griego *kryptos*, escondido y *graphein*, escribir, se define como un conjunto de técnicas cuya finalidad es actuar sobre los mensajes para transformarlos en representaciones incomprensibles para cualquier persona que no cuente con autorización para recibir la información.

Las ventajas y desventajas del uso de la criptografía se observan en la *tabla 4.1*.

Tabla 4. 1 Ventajas y desventajas del uso de la criptografía.

VENTAJAS	DESVENTAJAS
✓ Mantener la confidencialidad de la información. ✓ Preservar la integridad de la información logrando protegerla de los ataques a los cuales pueda ser susceptible. ✓ Utilizar códigos conocidos sólo por ciertas personas. ✓ Preservar la disponibilidad de la información cuando ésta sea requerida. ✓ Permite que la información utilizada por las organizaciones pueda manipularse de forma relativamente segura.	✓ Cuando se olvidan las técnicas empleadas para el proceso de cifrado puede perderse la información. ✓ Creación de nuevos algoritmos aun con las debilidades de algunos a falta de la creación de nuevos más robustos. ✓ Entre mayor robustez tenga un algoritmo de cifrado requiere capacidades mayores de cómputo.

Las dos operaciones fundamentales de la criptografía son el *cifrado* y el *descifrado*, estas operaciones integran los algoritmos de cifrado o también conocidos como algoritmos criptográficos, los cuales forman parte de la estructura de un sistema de cifrado que se muestra en la *figura 4.1* y se describe a continuación:

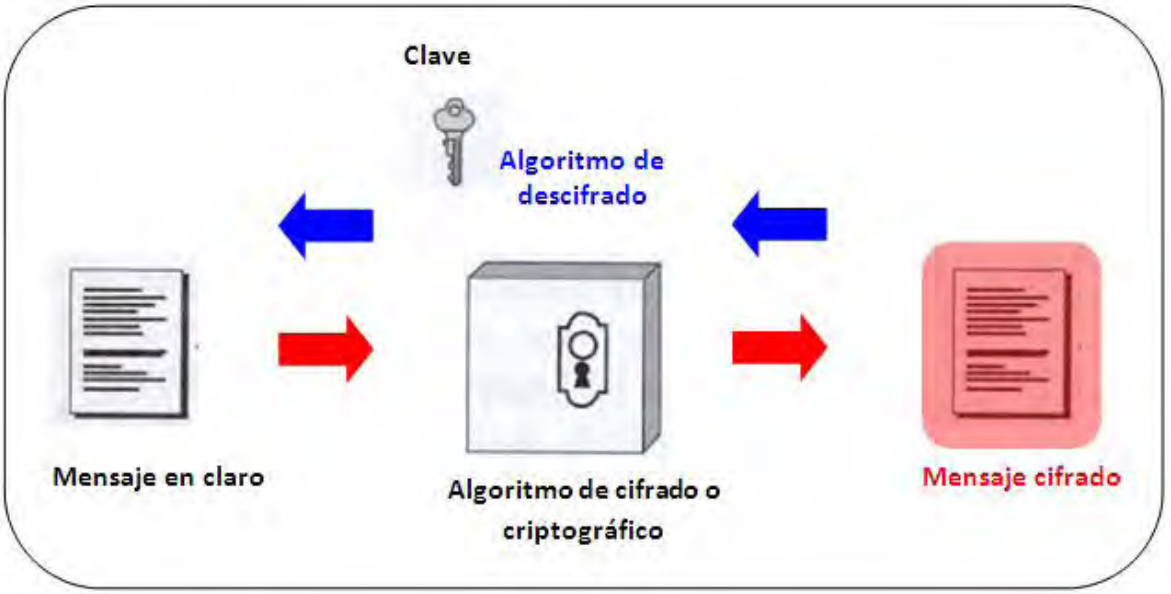

Figura 4. 1 Partes del sistema criptográfico.

Un sistema de cifrado es la transformación de un *mensaje en claro* en un *mensaje cifrado* utilizando un *algoritmo de cifrado, algoritmo de descifrado* y una *clave* los cuales se definen a continuación:

- ✓ *Algoritmo de cifrado o criptográfico:* son seleccionados considerando un conjunto de transformaciones para ser aplicadas al mensaje que se desea cifrar.

- ✓ *Clave o llave:* es un elemento fundamental en el cual radica la seguridad de un sistema de cifrado, es seleccionado considerando un espacio de todas las posibles claves, donde el tamaño de éste dependerá de las características y el tamaño requerido por la clave de cifrado.

- ✓ *Mensaje en claro o texto plano:* corresponde a la información cuya confiabilidad desea ser protegida, su tamaño y estructura dependerá del idioma, su alfabeto, las reglas para la construcción de oraciones y del criterio del propietario inicial o responsable de la información.

- ✓ *Mensaje cifrado o criptograma:* es el resultado de procesar el mensaje en claro utilizando el algoritmo de cifrado y la clave.

- ✓ *Algoritmo de descifrado:* conjunto de transformaciones aplicadas al criptograma con el objetivo de obtener el texto en claro.

Actualmente el uso de los sistemas de cifrado es altamente requerido para la protección de la información transmitida a través de las nuevas tecnologías con el objeto de preservar la integridad, la confidencialidad y disponibilidad ya que la seguridad de un sistema de cifrado debe depender ***únicamente*** de que la *clave utilizada sea secreta* y no de que el algoritmo de cifrado sea secreto.

b) Clasificación

Los sistemas de cifrado se clasifican tal como se observa en la figura 4.2:

Figura 4. 2 Clasificación de los sistemas de cifrado.

- Operaciones de transformación

Esta clasificación está relacionada con el tipo de operación utilizado para la transformación del mensaje en claro en mensaje cifrado. Todos los algoritmos de cifrado utilizan básicamente dos principios, la *sustitución* y la *transposición*, lo fundamental es que las operaciones utilizadas sean inversas para descifrar *(obtener el mensaje en claro a partir del mensaje cifrado)*.

La definición de las operaciones de transformación se observan en la tabla 4.2:

Tabla 4. 2 Operaciones de transformación.

SUSTITUCIÓN
Consiste en que cada elemento del mensaje en claro es cambiado por otro, para ello se requiere determinar la correspondencia entre las letras del mensaje y las letras del alfabeto en caso de ser el mismo u otro.
TRANSPOSICIÓN
Consiste en el reordenamiento de los elementos básicos del mensaje, letras, dígitos o símbolos.

Las operaciones de sustitución y transposición no son consideradas muy efectivas si son utilizadas de manera individual, sin embargo, son la base de sistemas robustos y difíciles de criptoanalizar[1].

- Tipo de procesamiento

Esta clasificación hace referencia a la forma en la cual es procesado el mensaje en claro, esto puede ser mediante un *cifrado por bloques* o *cifrado de flujo*.

- ✓ *Cifrado por bloques*: procesa un bloque de elementos produciendo un bloque de salida de tamaño moderado por cada bloque de entrada.

  La transformación utilizada siempre es la misma y depende únicamente de la clave.

  En este tipo de cifrado es imposible introducir bloques extraños sin que éstos sean detectados.

  Se tiene una velocidad de cifrado baja ya que es necesario leer previamente el bloque completo.

[1] **Criptoanalizar:** Es la acción de analizar un mensaje cifrado para obtener el mensaje en claro sin conocer el método de cifrado utilizado. El principal objetivo del criptoanálisis es la obtención de la clave utilizada por el sistema de cifrado.

Además tiene el inconveniente de ser propenso a errores de cifra, ya que un error se propagará por todo el bloque.

- ✓ *Cifrado de flujo*: el procesamiento de los elementos de entrada es de forma continua, lo que da como resultado la salida de un elemento cada vez. La forma en la cual se transforma el mensaje es carácter a carácter siendo la transformación diferente cada vez.

  La velocidad de cifrado es alta ya que no considera más que el elemento actual para operar.

  Tiene resistencia a errores ya que la cifra es independiente en cada elemento.

  Es vulnerable porque los elementos pueden ser alterados por separado.

La figura 4.3 ilustra el funcionamiento del cifrado por bloques y de flujo.

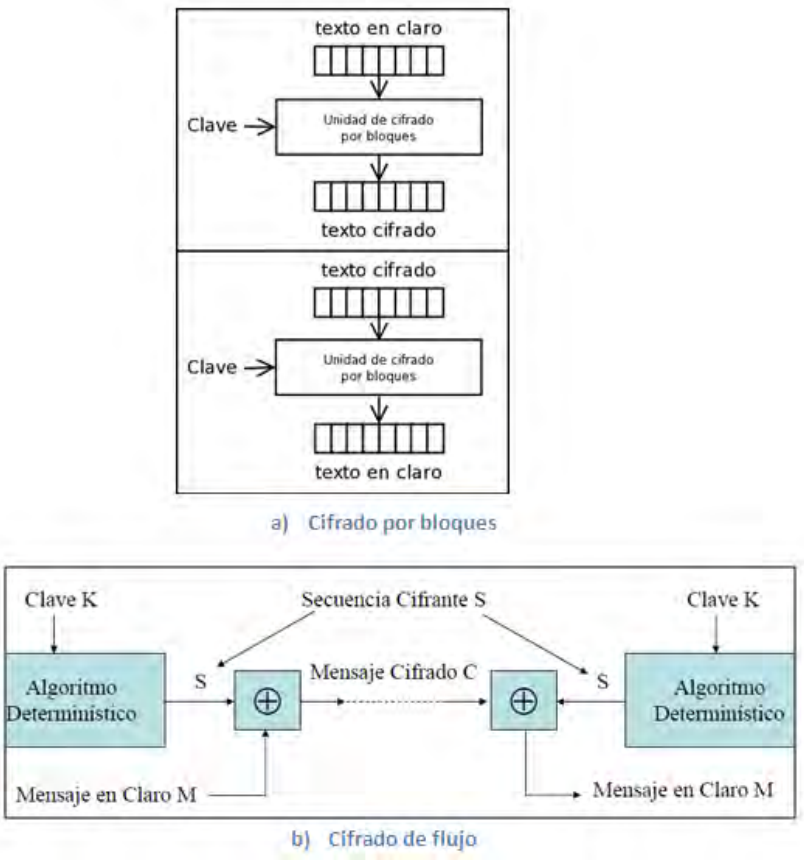

Figura 4. 3 a) Cifrado por bloques, b) Cifrado de flujo

- Número de claves utilizadas

Esta clasificación considera el número de claves utilizadas por el emisor y el receptor, es decir, si tanto el emisor como el receptor usan la **misma clave**, el sistema se denomina *simétrico*, de *clave única*, de *clave secreta* o *cifrado convencional*. Por otro lado, si el emisor y receptor utilizan cada uno **claves diferentes**, el sistema es denominado *asimétrico*, de *dos claves* o *cifrado de clave pública*.

- ✓ *Cifrado simétrico*: Este tipo de cifrado consiste en que ambas partes (emisor y receptor) compartan la misma clave para cifrar y descifrar denominada como *clave secreta* la cual será conocida únicamente por las partes involucradas. Este tipo de cifrado es rápido y es recomendable para cifrar grandes volúmenes de datos, es sencilla su implementación debido a que en su diseño emplea operaciones elementales.

  La confianza en su uso e implementación radica en el secreto de la clave, si el canal mediante el cual se transmite es inseguro, el cifrado es vulnerable y permite a los intrusos conocer la clave y con ello lograr descifrar el mensaje, logrando así conocer la información que contiene el mensaje en claro.

  La *figura 4.4* ilustra las partes que integran el cifrado simétrico.

  - Mensaje en claro.
  - Algoritmo de cifrado.
  - Clave privada.
  - Mensaje cifrado.
  - Algoritmo de descifrado.

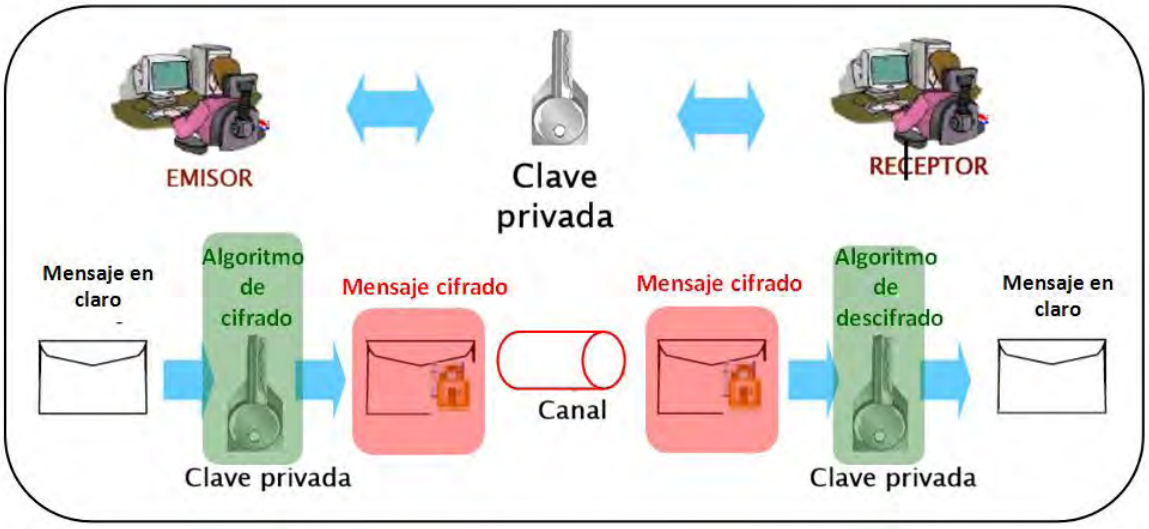

Figura 4. 4 Cifrado simétrico.

Los principales algoritmos simétricos se muestran en la tabla 4.3.

Tabla 4. 3 Algoritmos simétricos.

Nombre del algoritmo	Descripción
IDEA	*International Data Encryption Algorithm* (Algoritmo Internacional para el Cifrado de Datos). Fue creado por Xuejia Lai y James L. Massey y descrito por primera vez en 1991. Este algoritmo emplea tamaños de bloque de 64 bits y una clave de 128 bits. El número de rondas que utiliza son 8.5. Este algoritmo se diseñó como una sustitución del algoritmo DES pero como una actualización de PES Proposed Encryption Standard (*Estándar de Cifrado Propuesto*). Originalmente fue nombrado IPES Improved Proposed Encryption Standard (*Estándar de Cifrado Propuesto Mejorado*). IDEA emplea tres operaciones en su proceso de cifrado las cuales son: ✓ Operación XOR bit a bit ✓ Suma módulo 2^{16}. ✓ Multiplicación módulo 2^{16} M ✓ Su seguridad se basa en las distintas operaciones XOR bit a bit.

DES y 3DES	*Data Encryption Standard* (Estándar para el Cifrado de Datos). Fue creado en 1977 por IBM. Utiliza un cifrado en bloque en donde la longitud de éste es de 64 bits y la longitud de la clave es de 56 bits. El procedimiento para cifrar consiste en los siguientes pasos: ✓ El mensaje de 64 bits pasa a través de una permutación inicial. ✓ El algoritmo consiste en 16 iteraciones de la misma función, la salida de la iteración 16 contiene 64 bits en función de la entrada anterior y la clave, las mitades izquierda y derecha de la salida son intercambiadas para producir la presalida. ✓ La presalida pasa a través de una permutación que es el inverso de la función de permutación inicial para producir el texto cifrado de 64 bits. ✓ En relación a la clave de 56 bits se realizan permutaciones sobre la clave inicial y para cada una de las iteraciones se genera una subclave (K_i), las cuales serán el resultado de corrimientos a la izquierda y permutaciones. Por otro lado, el 3DES recibe este nombre porque consiste en hacer tres veces el procedimiento del algoritmo DES, fue desarrollado en 1978 por IBM. El 3DES fue creado para incrementar el tamaño de la clave sin necesidad de cambiar el algoritmo de cifrado, logrando con ello incrementar la seguridad del ya utilizado DES.
RC4	*Rivest Cipher 4 (Cifrado de Rivest 4)*, también conocido como ARC4 es un algoritmo de cifrado de flujo, fue diseñado por Ron Rivest en 1987. Para cifrar se combina el mensaje en claro usando la función XOR, se emplea una permutación de todos los 256 posibles símbolos de un byte de longitud, la permutación se inicializa con una clave de longitud variable entre 40 y 256 bits.

AES	*Advanced Encryption Standard* (Estándar de Cifrado Avanzado). Publicado por el NIST[2] en 2001 con la finalidad de sustituir al algoritmo de cifrado DES. En 1997 el NIST convocó al desarrollo de un nuevo algoritmo que fuese la base de un nuevo estándar, los requerimiento que este nuevo algoritmo debía cumplir eran: ✓ Ser un algoritmo de cifrado simétrico. ✓ Algoritmo de cifrado en bloques. ✓ Manejo de bloques de 128 bits. ✓ Soporte de manejo de claves de diferentes longitudes. ✓ Claves de 128, 192 y 256 bits. El algoritmo seleccionado para AES es "Rijndael" desarrollado por dos criptógrafos belgas: ✓ Dr. Joan Daemen ✓ Dr. Vincent Rijmen Cada ronda en este algoritmo se compone de cuatro transformaciones o funciones bien definidas: ✓ *SubBytes:* encargada de la sustitución de bytes. ✓ *ShiftRows:* recorre los renglones. ✓ *MixColumns:* se encarga de la mezcla de columnas. ✓ *AddRoundKey:* realiza la suma clave de ronda. La ronda final es idéntica a la transformación de ronda normal, excepto que se omite el paso encargado de la mezcla de columnas. AES hace uso de matemáticas polinomiales en estructuras de campos finitos.

✓ *Cifrado asimétrico:* este tipo de algoritmos está basado en funciones matemáticas y no en simples operaciones sobre los patrones de bits, ésta es la razón por la que los algoritmos son más lentos y el tamaño de las claves mayor, en comparación con los algoritmos de cifrado simétrico.

[2] **NIST** National Institute of Standards**:** Instituto Nacional de Estándares y Tecnología

En este tipo de cifrado se usan *dos claves* diferentes, una *clave pública* que se emplea para el *cifrado* de la información y la *clave privada* para realizar el proceso de *descifrado*.

El cifrado asimétrico es recomendado para autenticación, distribución de claves de sesión y firmas digitales.

La seguridad de este método de cifrado radica en el secreto de la clave privada la cual debe ser utilizada única y exclusivamente por el propietario de la misma ya que la clave pública es accesible para cualquier persona y no es necesario mantenerla oculta.

La *figura 4.5* ilustra las partes que integran el cifrado asimétrico.

- Mensaje en claro.
- Algoritmo de cifrado.
- Clave privada.
- Clave pública.
- Mensaje cifrado.
- Algoritmo de descifrado.

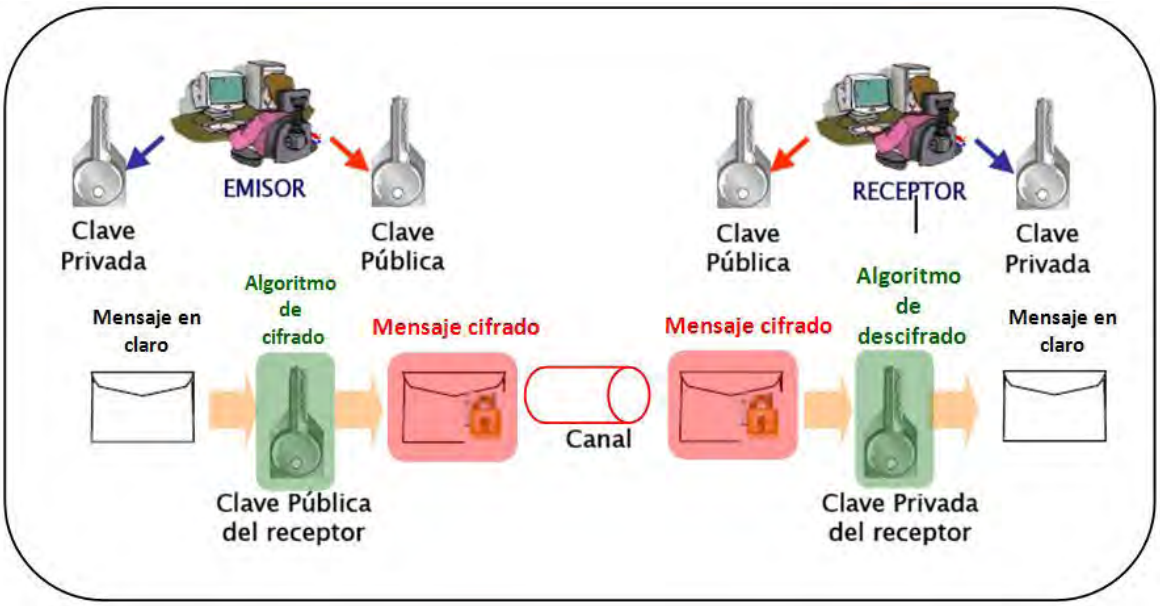

Figura 4. 5 Elementos que integran el cifrado asimétrico.

Los principales algoritmos asimétricos se muestran en la tabla 4.4.

Tabla 4. 4 Algoritmos asimétricos.

Nombre del algoritmo	Descripción
MD4 y MD5	*Message-Digest Algorithm 4* (Algoritmo de Publicación de Mensaje 4) y *Message-Digest Algorithm 5* (Algoritmo de Publicación de Mensaje 5). Los algoritmos MD4 y MD5 fueron desarrollados por Ron Rivest siendo MD4 la base que impulsó el desarrollo de MD5 en 1991 después de que Hans Dobbertin descubriera su debilidad. Utilizando el algoritmo de cifrado MD4 se realiza una manipulación de bits para obtener el valor hash[3], obteniéndolo de forma rápida, provocando que sea más riesgoso en un ataque. El cifrado MD5 se emplea con alta frecuencia en el mundo del software, con el objetivo de proporcionar la seguridad en relación a la integridad de la información manipulada, evitando con ello la infección por algún tipo malware[4]. La codificación del MD5 de 128 bits es representada típicamente como un número de 32 dígitos hexadecimal y la obtención del valor hash es lenta pero considerada más segura.
SHA	*Secure Hash Algorithm* (Algoritmo de Hash Seguro). Fue diseñado por NIST y NSA[5] en 1993, está basado en MD4 y MD5, fue revisado en 1995 dando lugar a SHA-1, tiene una entrada de longitud menor a 2^{64} bits y una salida de 160 bits. Las variantes del SHA cuyas diferencias se basan en un diseño modificado y rangos de salida incrementados, tal es el caso de **SHA-224**, **SHA 256**, **SHA 384** y **SHA-512** denominados a todos éstos **SHA-2**.

[3] **Hash:** Es el resultado de una función o algoritmo para generar claves que representa de manera casi unívoca a un documento, registro, archivo.
[4] **Malware:** software cuyo objetivo es infiltrarse en un sistema y causar daño en una computadora sin el conocimiento de su dueño.
[5] **NSA** National Security Agency: Agencia de Seguridad Nacional de los Estados Unidos.

RSA	Es un algoritmo de clave pública desarrollado en 1977, en el MIT[6] por Ronald *Rivest*, Adi *Shamir* y Leonard *Adelman*. Las letras iniciales de sus apellidos son el origen del nombre RSA. En 1983 el MIT patentó el algoritmo y la patente expiró el 21 de septiembre de 2000. Este popular algoritmo se basa en el problema matemático de la factorización de números grandes, las claves son de tamaño variable y se recomienda utilizar claves no menores de 768 bits, donde el número de bits debe ser lo suficientemente grande como para ser altamente compleja su factorización. El algoritmo de cifrado RSA resuelve el problema de la distribución de claves, puede ser utilizado en las firmas digitales[7]. Las desventajas del uso de RSA es que la seguridad de éste depende de la eficiencia computacional, además se requiere mayor tiempo de ejecución en comparación con el cifrado simétrico y la llave privada debe ser cifrada por algún algoritmo simétrico.
DIFFIE-HELMAN	Fue desarrollado en 1975 por *Whitfield Diffie* y *Martin Hellman* este algoritmo basa su seguridad en la dificultad para computar logaritmos discretos, lo que incrementa su efectividad. Es un algoritmo para el intercambio seguro de claves entre dos partes que previamente no han tenido contacto, empleando un canal inseguro. Matemáticamente se basa en las potencias de los números y en la función mod (módulo discreto). Uniendo estos dos conceptos se define la potencia discreta de un número como $Y = X^a \bmod q$. Si se considera el cálculo de potencias discretas éste resulta fácil pero el cálculo de la función inversa (logaritmo discreto), no cuenta con una solución analítica para números grandes.

[6] **MIT** Massachusetts Institute of Technology: Instituto Tecnológico de Massachusetts

[7] **Firma digital:** es un conjunto de datos asociados a un mensaje digital que permite garantizar la identidad del firmante y la integridad del mensaje.

4.2 Ventajas y desventajas de la implementación de sistemas de cifrado en las compañías aseguradoras

El uso de medios electrónicos para la transmisión, búsqueda, almacenamiento y manipulación de la información ha tenido un gran crecimiento con la aparición de Internet, sin embargo, de la misma forma en la cual ha evolucionado la tecnología, han surgido técnicas más sofisticadas para irrumpir en los servicios de seguridad (la confidencialidad, la autenticación, la integridad, el no repudio, el control de acceso y la disponibilidad), lo cual afecta a las organizaciones a nivel mundial y que a la vez representa uno de los principales frenos para la propagación del comercio electrónico.

Considerando a las compañías aseguradoras, las cuales son el objeto de estudio de este trabajo, la información que estas entidades gestionan, requiere una seguridad máxima debido a que los bancos de datos contienen información altamente confidencial de los clientes, tales como información médica, económica, situación familiar y en muchos casos resultados de informes confidenciales, considerando además que de forma frecuente dicha información será remitida a otras empresas (reaseguradores, ajustadores, empresas aseguradoras) razón por la cual es muy importante considerar los grandes beneficios que representa actualmente el uso de la criptografía como medida de protección para la información, cuya tendencia es cada vez más hacia el procesamiento y almacenamiento electrónico.

La protección de las bases de datos de las compañías aseguradoras es un asunto de gran importancia ya que la pérdida o alteración de la misma conllevaría a problemas financieros adversos que causarían no sólo el daño en el prestigio y credibilidad de la compañía sino hasta su desaparición.

La base de la protección utilizada por las compañías aseguradoras es el uso riguroso de la criptografía asimétrica (clave pública para cifrar, clave privada para descifrar), donde la clave pública estará a cargo de una persona confiable y responsable en cada empresa, el custodio de los datos, éste es la única persona facultada para poner en claro la información y quien entregará ésta a terceros, para ello el custodio debe documentar rigurosamente la entrega y sólo bajo instrucciones específicas por escrito.

La gran ventaja de que las compañías utilicen sistemas de cifrado asimétrico proporciona una mayor seguridad en la protección de la información por el uso de dos claves y la rigurosidad en que operan los algoritmos de cifrado, sin embargo, una de las desventajas

de estos sistemas es que debido al uso de operaciones matemáticas complejas requiere más recursos en cuanto a hardware. Por otro lado, si se considera la importancia de la información que se protege, no representa un gasto sino una inversión para las compañías.

En la actualidad han surgido nuevos mecanismos tecnológicos que proporcionan una seguridad más robusta, ejemplos claros son:

- ✓ *Certificados digitales:* consisten en una clave pública y un identificador o nombre de usuario del dueño de la clave, incluyendo el bloque firmado por una tercera parte confiable, denominada autoridad certificadora, en la que confía la comunidad de usuarios.

  Un usuario presenta su clave pública a una autoridad certificadora, la cual le proporciona un certificado que el usuario después podrá publicar

  Cualquier usuario puede obtener el certificado y verificar que éste es válido por medio de la firma fiable adjunta.

- ✓ *Firma electrónica:* su finalidad no es la confidencialidad de la información sino que el receptor se asegure de que el mensaje proviene del emisor correcto (autenticación). La firma electrónica funciona de la siguiente forma:

  - El emisor usa su clave privada para cifrar el mensaje.

  - Cuando el receptor recibe el texto cifrado, éste puede descifrarlo con la clave pública del emisor, demostrando de esta forma que el mensaje ha sido cifrado por él.

- ✓ *Cifrados híbridos:* en este tipo de cifrado se utiliza un cifrado simétrico en combinación con un asimétrico, esto es de la siguiente forma:

  - Se emplea el cifrado de clave pública para compartir una clave con el cifrado simétrico.

  - El mensaje enviado en el momento se cifra utilizando la clave y se envía al destinatario.

- Debido a que compartir una clave simétrica es inseguro, la clave utilizada para cada sesión es diferente.

El objetivo de la implementación de estos mecanismos es complicar cada vez más las labores intrusivas por parte de los atacantes, para lo cual la criptografía toma un papel fundamental e indispensable en la era digital y lo relacionado con la protección de las tecnologías de la información.

CAPÍTULO 5

Buenas prácticas para la protección de la información en las compañías aseguradoras

"La seguridad no es sólo un proceso tecnológico… es un proceso organizacional."

Autor desconocido.

5.1 Definición

Las buenas prácticas en el ámbito de la seguridad informática están integradas por un conjunto de políticas y normas específicas cuyo objetivo es la protección de los activos en una organización. Al ser implementadas ayudan a mitigar los principales problemas de seguridad a los que se encuentra expuesta, logrando como resultado mejorar su desempeño *(figura 5.1).*

Figura 5. 1 Objetivos de las buenas prácticas en las organizaciones.

En el caso particular de las compañías aseguradoras, la elaboración, la implementación y la difusión de las buenas prácticas contribuirá a la protección de la confidencialidad, disponibilidad e integridad de los datos confidenciales gestionados por estas entidades.

5.2 Buenas prácticas para la protección de la información confidencial de las aseguradoras

El conjunto de buenas prácticas definidas a continuación, considera un escenario general con relación a la manipulación de la información por las compañías aseguradoras y tiene por objetivo que éstas puedan ser aplicadas y ajustadas de forma particular considerando las necesidades y requerimientos de cada compañía.

Siendo la función de este conjunto de buenas prácticas una base sobre la cual las compañías aseguradoras puedan trabajar para establecer un conjunto de recomendaciones particulares a su organización dependiendo de sus procesos, sus actividades, su personal y los sistemas que intervengan en la manipulación de la información.

El escenario sobre el cual se trabaja se define a detalle en *la sección I de las buenas prácticas* que tiene por nombre ***Definiciones***.

Para el desarrollo de las secciones que integran las buenas prácticas se consideraron como modelo los controles especificados en el *anexo A de la norma ISO/IEC 27001:2005* y además las *Recomendaciones sobre medidas de seguridad aplicables a los sistemas de datos personales*, elaboradas por el IFAI (Instituto Federal de Acceso a la Información Pública) con base en ellos se estableció un modelo propio que contempla los controles mínimos requeridos para la protección de la información confidencial que es gestionada por las compañías aseguradoras.

Lo que da como resultado un conjunto de buenas prácticas generalizadas y aplicables a cualquier compañía aseguradora sin importar su tamaño o la forma en la cual es gestionada su información.

Las buenas prácticas están estructuradas en seis secciones las cuales se muestran en la figura 5.2 y se detallan más adelante:

Figura 5. 2 Secciones de las buenas prácticas.

I. Definiciones

Esta sección tiene por objetivo explicar a detalle cada uno de los conceptos y términos que son considerados en el escenario general de manipulación de la información confidencial por las compañías aseguradoras, el cual es ilustrado en la figura 5.3 y que servirá como base para definir los términos que intervienen en la gestión, proceso y almacenamiento de la información confidencial.

Figura 5. 3 Escenario general de la manipulación de la información por las compañías aseguradoras.

- ✓ *Compañía aseguradora:* es la organización que opera bajo el principio básico de la transferencia del riesgo, esto significa que la persona que contrata los servicios de la compañía realiza un pago determinado con base en ciertos factores, previendo la posibilidad de una pérdida o daño de gran magnitud hacia lo que desea proteger, ya sea hacia algo de valor material o hacia su propia vida o la vida de algún familiar (éste es el caso de los seguros de vida).

La redacción de estas buenas prácticas tiene como base el estudio de las compañías de seguro que trabajan las distintas opciones de seguro de personas, tal es el caso de los seguros de vida, los seguros de accidentes y los seguros de enfermedades.

Cabe resaltar que el conjunto de buenas prácticas creado puede ser acoplado a cualquier tipo de compañía aseguradora sea cual fuere la opción de su competencia *(seguros de personas, de accidentes, de enfermedades)*, sin embargo se da un mayor énfasis en su aplicación relacionada con la opción de seguros de personas debido al alto riesgo que representa la información manipulada, tal es el caso de expedientes médicos, dictámenes, estados de salud los cuales requieren controles de protección más estrictos.

- ✓ *Agente:* es aquella persona, empleado de la compañía aseguradora, que interviene en la contratación de seguros mediante el intercambio de propuestas y asesoramiento que permita satisfacer las necesidades de los contratantes.

- ✓ *Candidato:* es aquella persona que analizando sus necesidades solicita los servicios de la compañía aseguradora, siendo identificado como el posible cliente de la misma.

- ✓ *Propuesta:* es el documento elaborado por las compañías aseguradoras utilizado por el agente para obtener información personal de los posibles clientes además de incluir detalles relacionados con el tipo de seguro en el cual el candidato esté interesado.

- ✓ *Expediente del candidato:* contiene toda aquella información relacionada con el candidato que permite a la compañía aseguradora evaluar su caso (mediante la entidad que tenga asignada esta tarea) y determinar si le es otorgada o no la póliza que lo acreditaría formalmente como cliente con todos los derechos y obligaciones que esto conlleva.

- ✓ *Pruebas médicas:* son el conjunto de resultados de exámenes médicos o dictámenes requeridos por la compañía de seguros para evaluar el estado de salud de sus clientes o de los candidatos.

- ✓ *Capturista:* es la persona que recibe la propuesta y que se encarga de capturarla para obtener un documento digital dependiendo de la compañía, algunas de sus funciones serán digitalizar los documentos ya sea mediante la captura de la información en sistemas creados con este fin o la obtención de imágenes digitales de los documentos originales a partir de un escáner.

- ✓ *Clave pública del custodio:* es un conjunto de caracteres cuyo objetivo será permitir que el capturista pueda cifrar la información para protegerla, puede o no existir dependiendo de si la compañía aseguradora cuenta con algún método de cifrado implementado para la protección de su información.

- ✓ *Propuesta digitalizada:* es el documento elaborado por el capturista en donde están contenidos los datos del candidato.

- ✓ *Propuesta cifrada:* es el documento cifrado por el capturista utilizando la clave pública del custodio, en donde están contenidos los datos del candidato y demás información que está relacionada con el tipo de seguro de su interés. Puede o no la compañía contar con este documento dependiendo de si cuenta con un método de cifrado implementado en su organización.

- ✓ *Base de datos:* está integrada por el conjunto de información, (ya sea electrónica o documentos físicos) relacionada con los expedientes de los clientes o candidatos, documentos escaneados, propuestas de los clientes, resultados de exámenes médicos. Toda esta información puede o no estar protegida mediante algún método criptográfico.

- ✓ *Sistema de identificación anonimizado:* es el sistema que guarda las propuestas cifradas e información relacionada con los candidatos o clientes. Las compañías aseguradoras pueden contar o no con este sistema dependiendo de la forma en la cual almacenen su información.

- ✓ *Clave privada del custodio:* es un conjunto de caracteres cuyo objetivo será *(en combinación con la clave pública)* permitir que el custodio pueda poner en claro la información cifrada. Considerando que el esquema de protección implementado por la compañía sea el sistema de cifrado asimétrico.

- ✓ *Custodio:* es aquella persona quien es la responsable de poner la información cifrada en claro, ya que es la única que mediante su clave privada puede realizar dicha acción. Si la compañía aseguradora no cuenta con esta figura o un método de cifrado implementado, se considera que es aquella persona quien es la responsable de la protección de la información

- ✓ *Selección de riesgos:* consiste en la entidad centralizada o departamento *(dependiendo del tamaño de la compañía aseguradora)* encargado de evaluar el expediente del candidato para aprobar o rechazar su solicitud. Si al evaluar la propuesta el dictamen es favorable, se genera la póliza correspondiente que convertirá al candidato en cliente de la compañía.

- ✓ *Propuesta evaluada:* es el documento que contiene el dictamen de la compañía aseguradora la cual ha revisado previamente el expediente del candidato y la propuesta del mismo para determinar si es aceptado o no.

- ✓ *Propuesta en claro:* es el documento que contiene la información entendible.

Una vez determinadas las partes que intervienen en el proceso de gestión de la información confidencial se presenta el escenario general, considerado como ideal, pero a su vez está generalizado de tal forma que cualquier compañía aseguradora *(no importando su tamaño)* pueda considerar la implementación de determinados procesos y controles que le permitan optimizar la gestión de su información y con ello la seguridad en la misma.

El agente intercambia información relacionada con el tipo de seguro de su interés del candidato, éste a su vez proporciona información como datos personales y de contacto para que el agente pueda elaborar la propuesta, ésta forma parte del expediente del candidato y si es requerido se solicitan pruebas médicas. Toda la información del expediente que no sea digitalizada se resguarda en un archivo protegido que cuenta con controles de protección para que sólo el personal autorizado pueda tener acceso a esa información.

El *agente* lleva las propuestas de los candidatos a la compañía aseguradora para que los *capturistas* se encarguen de digitalizar los documentos creando la *propuesta* digitalizada la cual debe cifrarse con la *clave pública del custodio* y ya obtenida la *propuesta cifrada*, ésta es almacenada en el *Sistema de Identificación*

Anonimizado y a su vez también es enviada a *Selección de riesgos* quien es la entidad encargada de la aprobación de la propuesta para emitir la póliza correspondiente.

La propuesta digitalizada, debido a que no está cifrada, debe ser destruida para evitar que la información contenida sea vista por alguna persona no autorizada para ello.

Por otra parte el encargado de cuidar la información es el *custodio* quien tiene a su cargo una *clave privada* que le permite poner en claro la información, si el acceso a la información es realizado por varias personas se requiere considerar la implementación del *acceso basado en roles*[1].

Resultados esperados:

- ✓ Identificación de las partes que integran el escenario general de manipulación de la información confidencial de las compañías aseguradoras
- ✓ Comprensión de la característica de ***generalidad*** en el escenario y que permite su aplicación en cualquier compañía aseguradora sin importar su tamaño.

[1] **Control de acceso basado en roles:** regula el acceso de los usuarios a la información en términos de sus actividades y funciones de trabajo.

II. Seguridad física y del entorno

Esta sección contiene las medidas que deben considerarse para prevenir el acceso no autorizado a las instalaciones de la compañía para evitar pérdidas, tales como, robo, daño de los bienes e interrupción de las actividades del negocio.

A continuación se presenta un conjunto de recomendaciones generales *(aplicables a toda la organización)* y particulares (*consideraciones específicas a las etapas relacionadas con la manipulación de la información dentro de las compañías aseguradoras)*.

Generales:

- La compañía aseguradora debe implementar tarjetas de acceso para su personal y visitantes. O en su defecto, un libro de visitas que permita tener un control y registro del nombre, fecha, hora y asunto a tratar. Se recomienda que el personal a cargo de esta actividad solicite una identificación oficial para verificar que en efecto se trate de la persona registrada. Así como también la instalación de cámaras de video en puntos estratégicos de la organización.

- La compañía aseguradora debe implementar controles más rigurosos en las instalaciones de procesamiento de la información para permitir sólo el acceso al personal autorizado. Pueden considerarse controles de acceso más sofisticados como los lectores biométricos, las tarjetas RFID[2], los controles de acceso utilizando teclado o la combinación de alguno de éstos.

- Las instalaciones, así como el mobiliario de la compañía, deben encontrarse en condiciones óptimas tanto de estado como de limpieza que permitan reducir los riesgos a los cuales está expuesta la información cuando es manipulada.

- Es recomendable que la compañía aseguradora realice de forma periódica inventarios de su mobiliario y de archivos a su cargo, así como de los responsables, logrando con ello tener un control de la ubicación de la información reduciendo así la pérdida de la misma y mejorando la disponibilidad.

[2] **Tarjeta RFID** Radio Frequency IDentification**:** Identificación por radiofrecuencia, es un sistema de almacenamiento y recuperación de datos remotos que usa dispositivos denominados etiquetas, transpondedores o tags RFID. El propósito fundamental de la tecnología RFID es transmitir la identidad de un objeto (similar a un número de serie único) mediante ondas de radio.

- Con relación a las amenazas externas y ambientales, la compañía aseguradora deberá contar con medidas de protección física contra el daño por fuego, inundación, sismo, explosión, desastres naturales o hechos por el hombre que puedan causar algún tipo de destrucción dentro de la organización. Por ejemplo, contar con rutas de evacuación, salidas de emergencia, extinguidores, realización de simulacros para evacuar áreas, alarmas contra incendios, sistemas de enfriamiento para equipos que lo requieran, reguladores de voltaje, realizar mantenimiento periódico de los equipos para asegurar su continua disponibilidad e integridad.

- La compañía aseguradora debe informar a los empleados que éstos no deben sacar de las instalaciones de la organización equipos, información *(ya sea física o digital)* o software sin contar con alguna autorización para hacerlo.

Particulares:

Información a cargo del agente

- El agente deberá siempre portar la identificación que lo acredite como empleado de la compañía.

- El agente debe considerar las medidas de protección necesarias para el tratamiento de la información obtenida de los candidatos. Tal como el uso de carpetas para archivar y con ello evitar confusión de expedientes o la pérdida de la información.

- El agente deberá entregar la documentación recolectada en el tiempo y forma establecido por la compañía.

Información a cargo del capturista

- En el caso de que la compañía cuente con la figura del capturista o de no contar con ella, se considerará también el personal que recibe la información del agente y que a su vez interviene en el procesamiento de la información. Este personal deberá considerar las medidas de protección para la información que recibe, tales como el uso de archiveros, carpetas contenedoras de información, creación de expedientes para cada uno de los candidatos.

- Si la información que capturan o escanean se cifra, el personal que realiza esta tarea deberá tener precaución de no olvidar o extraviar la clave pública que le servirá para realizar dicha actividad.

- El personal que tiene contacto directo con la información no deberá consumir alimentos dentro de su área de trabajo con el objeto de proteger la integridad de los documentos a su cargo.

Almacenamiento y destrucción de expedientes

- Considerando el caso de que la información en estado físico (pruebas médicas, expedientes) sea archivada se recomienda que sea almacenada en una zona específica para esta actividad la cual tenga implementado algún control de acceso y medidas que protejan el estado y la disponibilidad de la información.

- La compañía aseguradora deberá considerar una sección de archivo muerto dentro del área de archivo, en el cual almacene aquellos expedientes que la organización haya determinado en desuso, improcedentes o sin importancia y éstos deberán ser destruidos en un tiempo no mayor a cinco años, donde la compañía deberá elegir la forma más adecuada y segura para su destrucción. Esto puede ser contratando empresas encargadas de proveer este servicio o empleando trituradoras de papel.

- En caso de que la información sea almacenada de forma electrónica en equipos de cómputo, se deberá considerar el centralizar el almacenamiento de la información en un servidor al cual mediante la asignación de claves de acceso y especificación de roles puedan acceder los empleados y realizar consultas, evitando con ello que la información confidencial se encuentre distribuida en los equipos de cómputo de la organización y pueda estar expuesta a cualquier copia, robo, modificación o simplemente no disponible cuando sea requerida.

- También puede considerarse cifrar la información contenida en el acervo digital y controlarla bajo un Sistema de Identificación Anonimizado, el cual permitirá que si la compañía aseguradora realiza intercambio de información con otras sucursales dentro del país éstas puedan acceder a la información y garantizar que es segura dicha transacción.

- En el caso de que los expedientes se archiven cifrados debe toda aquella información no cifrada ser destruida para evitar su exposición al personal no autorizado.

Información a cargo del custodio

- La compañía aseguradora deberá considerar qué documento es necesario para que el custodio o el personal a cargo de los expedientes pueda ya sea ponerlos en claro *(en el caso que la información esté cifrada)* o enviarlos a selección de riesgos *(quienes emiten la aprobación de la propuesta del candidato)* o una tercera entidad como lo es una reaseguradora.

Información a cargo de selección de riesgos

- Si la compañía aseguradora cuenta con esta área como una sección centralizada fuera de la organización, a la cual le son enviados los expedientes para su análisis, se debe considerar que los medios de transmisión de la información sean seguros ya sea mediante un servicio de mensajería privado y propietario de la compañía o utilizando medios electrónicos mediante la implementación de un Sistema de Identificación Anonimizado, al cual podrá acceder Selección de riesgos para la consulta de expedientes vía remota, dicho sistema contendrá todo el acervo de expedientes en formato digital que puede o no estar cifrado dependiendo de si la organización ha implementado o no algún método de cifrado.

- En el caso de tener implementado algún método de cifrado asimétrico se debe tener extremo cuidado con la asignación de claves privadas, considerando que las claves privadas en conjunto con la pública del custodio permiten poner en claro la información.

Resultados esperados:

- ✓ Mejorar los controles de seguridad física y del entorno que permitan proteger los lugares en los cuales la información es manipulada y almacenada.
- ✓ Considerar la implementación de algunas etapas dentro del proceso de gestión de la información de las compañías aseguradoras para mejorar la seguridad de la información.

III. Control de acceso

Esta sección considera aquello que está relacionado con el control de acceso a la información, la prevención de accesos no autorizados a los sistemas que la gestionan, las computadoras, la detección de actividades no autorizadas.

- La compañía aseguradora debe especificar y difundir una política en la cual especifique los controles de acceso que se implementarán para acceder a los sistemas y a la información confidencial de la organización. Si ésta es accedida por varios empleados es recomendable implementar el modelo de acceso basado en perfiles, el cual otorga una serie de permisos con base en lo que el perfil requiera y los usuarios son registrados dentro de un perfil considerando sus responsabilidades y capacidades, de esta forma los permisos son otorgados por perfiles y no a cada empleado de forma particular.

- La compañía aseguradora debe establecer un criterio para la asignación de contraseñas, el cual permita la generación de contraseñas robustas que protejan el acceso a los sistemas y a los equipos de la organización. En el caso de utilizar claves públicas o privadas, para cifrar éstas deben ser de igual forma robustas y deben ser protegidas por los propietarios de las mismas. Para la gestión de contraseñas y claves se pueden considerar las siguientes recomendaciones que se muestran en la tabla 5.1:

Tabla 5. 1 Recomendaciones para la gestión de contraseñas y claves

RECOMENDACIONES PARA GESTIÓN DE CONTRASEÑAS Y CLAVES
✓ Las contraseñas y claves deben renovarse frecuentemente, ya que una clave queda expuesta cada vez que se usa.
✓ Debe de contarse con claves y contraseñas diferentes para servicios diferentes (autenticación, transmisión, almacenamiento) y en el caso de las claves dependiendo si es pública o privada.
✓ Claves y contraseñas diferentes para cada persona o grupo, si no están autorizados para comunicarse entre sí no deben compartir la misma clave.
✓ Anulación de claves y contraseñas que han sido utilizadas por personas o grupos que ya no laboran dentro de la compañía, porque éstos ya no deben acceder a la

información.

- ✓ Para la creación de claves y contraseñas utilizar letras mayúsculas, minúsculas, caracteres especiales y números.
- ✓ Evitar siempre utilizar palabras de diccionario o que contengan información personal, como fechas, nombre de canciones, mascotas, familiares etcétera.
- ✓ Longitud mínima de ocho caracteres *(dos letras mayúsculas, dos letras minúsculas, dos números, dos caracteres especiales)*.
- ✓ Las claves y contraseñas no deberán ser divulgadas, deben ser fáciles de recordar y siempre tienen que mantenerse en secreto *(evitar colocarla en lugares visibles)*.

- Para evitar los accesos no autorizados a los equipos de cómputo, éstos deben contar con un sistema de bloqueo que al detectar que un usuario ingresa incorrectamente su contraseña en más de tres ocasiones, emita una alerta de bloqueo del equipo.

- El personal a cargo de los equipos deberá verificar de forma periódica que éstos cuenten únicamente con los servicios requeridos con base en sus actividades para evitar así puertos abiertos o puntos vulnerables que puedan ser utilizados para acceder a la información de la compañía.

- Para tener un control de las actividades y programas instalados, se recomienda establecer políticas para la instalación de software, en la cual se especifique bajo qué circunstancias estará permitida su instalación en los equipos de cómputo de la organización.

- La compañía aseguradora deberá establecer los usos de internet dentro de la organización con el objetivo de evitar que los empleados accedan a sitios ajenos a las actividades relacionadas con el negocio. Disminuyendo así los riesgos de visitar sitios web comprometidos o con códigos maliciosos que puedan dañar o afectar la continuidad de las actividades.

- La compañía aseguradora deberá definir los permisos de lectura y escritura en la información manipulada por los empleados con el objetivo de evitar que personas no autorizadas para ello puedan copiar, modificar o eliminar documentos.

- Considerando el caso de que las compañías aseguradoras permitan el acceso remoto de sus empleados a los sistemas o equipos que gestionan la información confidencial, se deberán especificar claramente controles para la autenticación e identificación que garanticen que la persona que accese cuente con la autorización para hacerlo.

Resultados esperados:

- ✓ Implementación de controles de seguridad para todos aquellos accesos a la información con el objetivo de proteger su confidencialidad, integridad y disponibilidad.

- ✓ Reducción de accesos no autorizados a equipos de cómputo, propiedad de la compañía aseguradora.

- ✓ Implementación del uso de contraseñas robustas en los usuarios y concientización de éstos del por qué es necesario el uso de ese tipo de contraseñas.

- ✓ Implementación del modelo basado en roles (considerando los requerimientos de la organización y de la forma en la cual es gestionada su información).

IV. Administración de incidentes de seguridad para la continuidad de la organización

Los objetivos de esta sección son contrarrestar las interrupciones de las actividades productivas, consideradas como críticas para la compañía aseguradora, evitar cualquier tipo de falla o desastre que ponga en riesgo la continuidad en las actividades o la disponibilidad de la información, cerciorar que la seguridad de los sistemas empleados para la gestión de la información puedan prevenir pérdidas, abusos, modificaciones de los datos, protegiendo con ello la integridad, la disponibilidad y la confidencialidad de la información.

- La compañía aseguradora debe establecer un plan de contingencia tanto preventivo como correctivo, los cuales le permitan mantener y recuperar las operaciones, lo que da como resultado que la información esté disponible en el tiempo requerido.

- En el caso de la información contenida en los equipos de cómputo, los servidores, los sistemas que almacenen información cifrada o no (dependiendo de la compañía aseguradora) o todos aquellos dispositivos que almacenen información deberán establecer los encargados de éstos, el uso de respaldos con el objeto de que ante cualquier evento extraordinario se tenga siempre disponible la información.

  Con relación a los respaldos de información, es recomendable hacer un primer respaldo que contenga toda la información de cada dispositivo, tal como información de los clientes, datos de los usuarios, las configuraciones del sistema, es decir, toda aquella información que no pueda ser recuperada de ninguna parte, una vez hecho esto, se debe hacer de forma periódica un respaldo de aquellos archivos que han sido modificados y cada uno de los dispositivos de almacenamiento que guarden los respaldos deben estar debidamente etiquetados con información clara pero no excesiva (ya que eso puede facilitar las tareas de un posible perpetrador).

  Las copias de seguridad no deben guardase únicamente cerca de los sistemas, ya que al presentarse cualquier tipo de desastre, podría ocasionar que tanto las copias como los sistemas queden totalmente inutilizables, tampoco es recomendable tenerlas a gran distancia de éstos, ya que podrían ser requeridas

en las operaciones diarias de la organización, de este modo se recomienda dejar un juego de copias cerca los sistemas y otro lejos.

- Se recomienda que los encargados de los sistemas que gestionan la información en las compañías aseguradoras realicen revisiones periódicas *(semanales o mensuales)* de las bitácoras, con el objeto de saber cómo está funcionando el sistema o para detección de alguna actividad intrusiva, la cual pueda representar un riesgo para la confidencialidad, disponibilidad y la integridad de la información.

- La compañía aseguradora debe destinar personal, para realizar tareas de mantenimiento a los sistemas que gestionan y almacenan la información, tales como computadoras, impresoras, escáneres. Con el objeto de contribuir a la disponibilidad de la información y con ello la continuidad en las operaciones de la organización.

- Todo el personal que gestiona la información de la compañía aseguradora, debe considerar la implementación de controles de seguridad para cada equipo a su cargo, como es el caso de las actualizaciones de seguridad para el software utilizado, el uso de antivirus, de firewall y sobre todo tener presente las diferentes técnicas de ingeniería social[3] que pueden ser aplicadas para obtener información de interés por parte de algún perpetrador.

- Es recomendable que la compañía aseguradora asigne personal que se encargue de elaborar reportes periódicos (semanales o mensuales) en los cuales se registren aquellos eventos que se han presentado o que representan un riesgo potencial para los sistemas y para la información. Esto contribuye para la mejora continua de los controles establecidos, dando como resultado la mejora en la seguridad de la información.

- Las compañías aseguradoras que aún no cuenten con un método de cifrado implementado como una medida de protección para la información, deben considerar las diferentes opciones tales como cifrado simétrico, asimétrico, híbrido, certificados y firmas digitales, funciones hash, curvas elípticas, lo cual representa alternativas para la protección de la información confidencial y que

[3] **Ingeniería social:** es la técnica especializada o empírica del uso de acciones estudiadas o habilidosas que permiten manipular a las personas para que voluntariamente realicen actos que normalmente no harían.

pueden ser ajustadas dependiendo de las necesidades requeridas por la organización.

Resultados esperados:

- ✓ Respaldos de la información manipulada por los sistemas de la compañía aseguradora.
- ✓ Tareas de mantenimiento periódico para los sistemas, dispositivos que tienen contacto directo o indirecto con la información confidencial, entre las tareas se considera la revisión de las bitácoras para garantizar que los equipos de cómputo y sistemas operan de manera satisfactoria.
- ✓ Considerar la implementación de algún sistema de cifrado dependiendo de las necesidades de la compañía aseguradora.
- ✓ Actualización de software (antivirus, firewall, IDS, parches de seguridad) en los cuales se tomen en cuenta los avances tecnológicos.

V. Seguridad de recursos humanos

Esta sección tiene como finalidad la reducción del riesgo producido por errores humanos tales como robo, fraude, abuso en el uso de la información, sistemas y equipos que la gestionan, además considera recomendaciones dirigidas al personal para concientizarlo con relación a las amenazas que afectan la seguridad de la información y en consecuencia a la continuidad de las actividades en la compañía aseguradora, por lo cual es necesaria su participación y apoyo hacia las políticas corporativas de seguridad en contra de accidentes o fallas.

Esta sección se subdivide a su vez en tres subetapas que se describen a continuación:

- ✓ *Antes de la contratación:* se considera esta subetapa cuando el área de recursos humanos de la compañía aseguradora contrata personal al cual le especifica las actividades a realizar dentro de la organización y a su vez lo relacionado con su contratación *(contrato, rol, responsabilidades, horario, verificación de antecedentes etcétera)*.

- ✓ *Durante la contratación:* esta subetapa corresponde a cuando el nuevo personal ha sido contratado por la compañía aseguradora y desempeña un conjunto de actividades que son remuneradas por la organización.

- ✓ *Finalización de la contratación:* esta subetapa considera cuando el personal deja de prestar sus servicios dentro de la compañía aseguradora, ya sea por cuestiones voluntarias del personal, decisión de la organización, jubilación o pensión.

Antes de la contratación

- La compañía aseguradora debe definir claramente los roles y las responsabilidades de los puestos en los cuales contratará nuevo personal, es recomendable que la organización documente cada uno de los roles y las responsabilidades de los puestos que la conforman, de esta forma el personal que desee incorporarse a la compañía conocerá claramente esta información relacionada con el puesto de su interés.

- La compañía aseguradora a través de su departamento de recursos humanos, deberá realizar la selección cuidadosa de su personal, considerando antecedentes, referencias, habilidades, conocimientos *(dependiendo el puesto para el cual se incorpore)*. Una vez que el personal sea incorporado es necesario definir a qué información estará autorizado para acceder y los riesgos que implica.

- Es indispensable que los aspirantes conozcan claramente los términos y las condiciones del empleo que solicitan, los cuales deberán ser acordados y firmados considerando los términos y las condiciones con relación a los contratos de trabajo emitidos por la compañía aseguradora. En este documento se deben expresar las responsabilidades que asume el empleado con relación a la seguridad de la información de la organización.

Durante de la contratación

- Es responsabilidad de la parte directiva de la compañía aseguradora requerir que sus empleados sigan todos aquellos controles implementados para la seguridad de la información, considerando todas aquellas políticas y procedimientos establecidos

- La compañía debe proporcionar a sus empleados actualizaciones regulares y pláticas para la toma de conciencia que contribuyan a fomentar la cultura de seguridad informática y la importancia de ésta en las actividades desarrolladas en su trabajo.

- Es necesario que la compañía aseguradora establezca un proceso disciplinario formal, del cual sean notificados todos empleados y que considere las acciones a seguir en consecuencia del incumplimiento de alguna medida de seguridad informática previamente establecida.

Finalización de la contratación

- La compañía aseguradora debe establecer claramente cuáles serán las responsabilidades para que el empleado lleve a cabo la terminación de sus actividades dentro de la organización.

- La compañía aseguradora debe definir cuáles son las actividades que el empleado realizará para la devolución de activos de la organización en su

posesión, una vez concluidas sus actividades, el contrato o acuerdo con la organización.

- La compañía aseguradora debe retirar a todos los ex empleados, los derechos de acceso a la información y los recursos para el procesamiento de ésta, *(contraseñas, cuentas de usuario en sistemas, dirección de correo electrónico)*, en un periodo no mayor a veinticuatro horas después de haberse presentado la baja del empleado de la compañía aseguradora.

Resultados esperados:

- ✓ Garantizar que todo el personal que labora en la compañía aseguradora sea confiable y que el área de recursos humanos lleve a cabo procedimientos rigurosos en la selección del personal cuando se efectúen contrataciones.
- ✓ Que el personal cuente con capacitaciones periódicas y pláticas de concientización para contribuir a la implementación y al buen funcionamiento de los controles de seguridad informática con los que cuenta la organización.
- ✓ Concientización de todo el personal que labora en la compañía aseguradora que contribuya a crear una cultura de seguridad informática aplicada en la preservación de la continuidad del negocio.

VI. Cumplimiento y políticas de seguridad

Esta etapa provee la directriz y el soporte de las autoridades para regular las actividades relacionadas con la gestión de la seguridad de la información, debe tomar en consideración los requisitos de la compañía aseguradora, las leyes y los reglamentos pertinentes.

Esta etapa a su vez considera puntos relacionados con el cumplimiento de leyes, estatutos, obligaciones reglamentarias, contractuales vigentes relacionados con la seguridad de la información.

Con relación a la redacción de políticas de seguridad de la información, éstas definen los requerimientos de seguridad de la compañía, los procedimientos para detectar, prevenir y responder a incidentes de seguridad además de su uso aceptable, de esta forma la compañía aseguradora contará con un marco para reforzar la seguridad de la información.

- La compañía aseguradora debe considerar que las políticas vigentes o las que estén en proceso de elaboración cumplan con las siguientes reglas especiales que se muestran en la *tabla 5.2.*

Tabla 5. 2 Reglas especiales para políticas de seguridad

REGLA	DESCRIPCIÓN
Mínimo privilegio	Consiste en no asignar más privilegios a un empleado de aquellos que sean requeridos para desempeñar sus actividades
Flexibilidad	Se refiere a la "debilitación" de controles sobre algún empleado o proceso para poder llevar a cabo sus actividades
Separación de funciones o roles	Hace mención de no proporcionar demasiado poder a un empleado al asignarle muchas funciones.

- Las políticas establecidas por la compañía aseguradora deben estar respaldadas por la dirección, además deben ser conocidas y aprobadas por los empleados, si

esto no se cumple no pueden ser responsabilizados por incurrir en alguna violación de las mismas.

- La compañía aseguradora debe considerar medios para la difusión en la organización de las políticas de seguridad, mediante el uso de carteles, correos electrónicos, trípticos, videos o juntas informativas. Es sumamente importante que todo el personal tenga conocimiento de las políticas de la compañía y la importancia de éstas para regular las actividades.

- Es necesario que la compañía aseguradora se mantenga actualizada con relación a las leyes, los estatutos, los estándares, las obligaciones tanto reglamentarias como contractuales de ésta con otras entidades (nacionales, internacionales), con sus empleados y que aquella información que deba ser del conocimiento de éstos sea difundida.

- La compañía aseguradora debe cerciorarse que los sistemas que utiliza cumplan con las políticas y estándares de seguridad vigentes.

- Las políticas deben ser redactadas de forma clara, sin ambigüedades, ni tecnicismos, además deben definirse claramente los objetivos, al considerar estos puntos, las políticas de seguridad podrán ser entendidas por todo el personal que integra la compañía aseguradora y se conseguirán mejores resultados en la aplicación dentro de la compañía.

Resultados esperados:

- ✓ Actualización de la compañía aseguradora con relación a las leyes, los estatutos, los estándares, las obligaciones reglamentarias y contractuales vigentes.
- ✓ Contar con políticas de seguridad como una directriz para el soporte de las actividades dentro de la compañía.
- ✓ Considerar la difusión adecuada de las políticas de seguridad para todo el personal que la integre, así como también contar con el apoyo de la parte directiva para la aprobación de las mismas.

CONCLUSIONES

El conjunto de buenas prácticas resultado de este trabajo de investigación, tiene por objeto servir como base para que cada compañía aseguradora pueda redactar un conjunto personalizado de buenas prácticas que considere la forma en la cual es manipulada su información, los procesos específicos con los que cuenta implementados actualmente, los requerimientos en el ámbito de la seguridad de la información y los recursos económicos destinados para su inversión. Y de esta forma puedan mejorar la confidencialidad, la integridad y la disponibilidad de su información mediante la implementación de controles de seguridad en la organización.

Cabe hacer mención que actualmente se cuenta con diversas opciones para mejorar la seguridad en la transmisión, manipulación y almacenamiento de la información utilizando medios electrónicos, como lo son los certificados y firmas digitales, las funciones hash, las curvas elípticas, los métodos de cifrado híbridos, entre otras alternativas que las compañías aseguradoras pueden implementar tomando en cuenta la evaluación de sus recursos y las necesidades de protección de sus activos.

El considerar estas opciones y la creación de un *Sistema de Identificación Anonimizado* quedan como alternativas abiertas que en conjunto con la implementación de buenas prácticas y políticas de seguridad, permitirán a las compañías aseguradoras asegurar a sus clientes que la información que proporcionan y que a su vez integra los expedientes, cuenta con los controles indispensables para garantizar la seguridad de la información.

Además la creación de políticas de seguridad y buenas prácticas en las compañías aseguradoras contribuirán a todas aquellas iniciativas legales que actualmente se trabajan en México para la creación de una ley a nivel constitucional que permita proteger la información sensible como lo son los datos personales, los expedientes y dictámenes médicos, estados financieros, entre otros documentos y lograr que no sólo sea aplicado al sector público a través de entidades como el IFAI, sino la inclusión del sector privado al cual pertenecen las compañías aseguradoras.

Por último, cabe destacar que el contenido de este trabajo de investigación fue diseñado para proporcionar un buen acercamiento con el lector en sus diferentes variedades, desde aquellos que no cuentan con grandes conocimientos en el área de la seguridad informática, hasta aquellos especializados en estos temas, todo ello con el objetivo de lograr la difusión de un tema tan importante como actualmente lo es y será para futuras generaciones la seguridad de la información.

APÉNDICES

APÉNDICE A

TIPOS DE CÓDIGOS MALICIOSOS

Un código malicoso es un software que tiene por objetivo lograr el acceso no autorizado a un sistema de cómputo, aprovechando la presencia de ciertas vulnerabilidades que le permitan acceder a un sistema, ya una vez dentro, este código busca violar las reglas previamente establecidas por los administradores o usuarios, para de esta forma lograr comprometer al equipo y volverlo aún más vulnerable.

Dentro de las principales tareas de un código malicioso son:

- ✓ Propagación por los equipos que integren la red o que naveguen en Internet.
- ✓ Robo de información sensible e importante para la organización o usuarios como claves de acceso, documentación confidencial, etcétera.
- ✓ Atentar contra la disponibilidad de la información.
- ✓ Causar molestia a los usuarios disminuyendo la eficiencia de los recursos empleados.

Los tipos de códigos maliciosos más populares se mencionan a continuación:

a) Caballo de Troya

Conjunto de instrucciones escondidas dentro de un programa de forma tal que parezca realizar acciones esperadas por el usuario pero que realmente realiza otro tipo de funciones con el objeto de comprometer la seguridad del sistema.

b) Gusano

Es un programa que tiene por objeto propagarse entre los equipos informáticos aprovechando los recursos necesarios para hacerlo, de esta forma se replica a sí mismo cuando así lo requiere.

Para su propagación entre computadoras emplea conexiones de red y dentro de sus objetivos más comunes son el robo, la destrucción y modificación de la información contenida en el host víctima.

c) Virus

Son programas creados con el objetivo de interferir en el funcionamiento de un sistema de cómputo, dañando o eliminando información a menudo con el propósito de disminuir la rapidez de las operaciones y a la vez buscar problemas en los procesos para causar daños en la seguridad del sistema.

APÉNDICE B

CONCEPTOS RELACIONADOS CON AMENAZAS DE TIPO HUMANO.

Debido a la confusión y al mal uso de algunos términos relacionados con los diferentes tipos de ejecutores de ataques informáticos, los cuales se han diferenciado por los objetivos y los medios empleados para llegar a éstos, dichos conceptos se detallan a continuación:

- ✓ HACKERS: Esta palabra es empleada para referirse a una persona experta en una determinada rama o técnica relacionada con las tecnologías de la información, a su vez, también puede definir a aquella persona que siente cierto apasionamiento por descubrir o adquirir conocimientos relacionados con cosas nuevas, entendiendo el funcionamiento de las mismas.

- ✓ CRACKERS: Conocidos como (rompedores) o "Black hat" (sombreros negros), que emplean sus conocimientos con fines maliciosos, dejando atrás toda moral, e incluso con fines bélicos, ejemplo de los ataques de un cracker son:

  - Intrusión de redes.
  - Acceso ilegal a sistemas gubernamentales.
  - Robo y modificación de información.
  - Distribución de material ilegal o moralmente inaceptable.
  - Piratería.
  - Fabricación de virus y de herramientas de crackeo.

  La diferencia entre un hacker y un cracker es en cuanto a valores morales, sociales y políticos, puesto que el primero únicamente busca el conocimiento como pasión y el segundo lo ve como una herramienta para la destrucción.

- ✓ BUCANEROS o PIRATAS: Se trata en realidad de comerciantes. Los bucaneros venden los productos crackeados como tarjetas de control de acceso de canales de pago. Por ello, se considera que los bucaneros no existen en la red, únicamente se

dedican a explotar este tipo de tarjetas para canales de pago que los crackers crean. Los bucaneros suelen ser personas sin ningún tipo de conocimientos ni de electrónica, ni de informática, pero con amplios conocimientos de negocios. El bucanero compra al *CopyHacker* (tipo de hacker que se dedica a clonar piezas electrónicas y altera el funcionamiento de distintas piezas que hay en el mercado) y revende el producto bajo un nombre comercial.

- ✓ NEWBIE: En un principio se empleó el término para describir a una persona principiante que se adentraba en un campo de la computación, siendo comúnmente empleado para indicar a usuarios de internet de prominente práctica pero de corto conocimiento técnico a un recién llegado a un foro o comunidad. Después el empleo de esta palabra se ha extendido para indicar a un recién llegado a cualquier grupo específico.

- ✓ PHREAKER: Son aquellas personas que investigan y estudian el funcionamiento de los sistemas telefónicos mediante el uso de tecnología por el placer de manipular un sistema tecnológicamente complejo y en ciertas ocasiones también para poder obtener algún tipo de beneficio como llamadas gratuitas.

- ✓ LAMERS: Aplicado a aquellas personas como producto de una falta de madurez, sociabilidad o habilidades técnicas, hace que se le considere incompetente en una cierta materia o actividad específica o dentro de un grupo o comunidad aunque lleve un tiempo más que prudente, para aprender sobre la materia, actividad o adaptarse al grupo o comunidad que le considera un lammer.

- ✓ SRIPTKIDDIE: Un cracker inexperto que usa programas, scripts, exploits, troyanos, nukes, que son creados por otros, con la finalidad de romper la seguridad de un sistema. Este tipo de personas suele presumir de ser un hacker o cracker cuando en realidad no posee un grado relevante de conocimientos.

- ✓ SPAMMERS: Son aquellas personas, que se dedica a la distribución o presentación de spam (correo o mensajes considerados basura).

- ✓ TRASHING: Aquellas personas que obtienen información por medio de la búsqueda en los basureros con el objeto de encontrar información que pudiera resultar importante.

GLOSARIO

A	
Activo	Es el conjunto de bienes que tienen un determinado valor para una organización y los cuales deben ser salvaguardados debido a la importancia que han adquirido.
Amenaza	Es todo aquello que pretende causar destrucción o daño.
Ataque	Es la explotación por medio de una amenaza, de una vulnerabilidad detectada.
B	
Bomba lógica	Programa informático que se instala en un equipo, permaneciendo oculto hasta cumplirse las condiciones determinadas para su activación y con ello ejecutar las acciones para las cuales fue creada.
BSI British Standard Institute	Instituto del Estándar Británico
Bucanero	Comerciantes que venden productos crackeados, estas personas carecen de conocimientos de electrónica e informática.
C	
Caballo de Troya	Programa malicioso que da la apariencia de ser benigno con lo cual consigue acceso al sistema con el objeto de comprometer la seguridad del mismo.
Ciclo Deming o ciclo PDCA (Plan Do Check Act)	(Planificar, Hacer, Verificar, Actuar) es una estrategia de mejora continua de la calidad en cuatro pasos, basada en un concepto ideado por Walter A. Shewhart. También se denomina espiral de mejora continua. Es muy utilizado por los Sistemas de Gestión de Seguridad de la Información (SGSI).
Código malicioso	Software que accede a un sistema de cómputo sin autorización intentando violar las reglas previamente establecidas hasta lograr comprometerlo.

Control de acceso basado en roles	Regula el acceso de los usuarios a la información en términos de sus actividades y funciones de trabajo.
Cracker	Persona que accede a un sistema de cómputo ajeno sin contar con autorización y realiza acciones que dañan el sistema.
Criptoanalizar	Es la acción de analizar un mensaje cifrado para obtener el mensaje en claro sin conocer el método de cifrado utilizado. El principal objetivo del criptoanálisis es la obtención de la clave utilizada por el sistema de cifrado mediante medios ilícitos.
D	
Dato	Conjunto de caracteres, letras números que no tienen significado alguno, debido a que no han sido sujetos a ningún análisis.
Denegación de servicio	Término que por sus siglas en inglés se denomina DOS (Deny of Service), el cual hace referencia al tipo de ataque, que consiste en la imposibilidad de acceso a un recurso o servicio por parte del usuario legítimo.
DoD Department of Defense	Departamento de Defensa de los Estados Unidos
DOS Disk Operating System	Sistema Operativo de Disco, utilizado por las computadoras personales.
E	
Entorno de seguridad	Delimitación del área que contiene los activos que requieren protección de intrusos o agentes que puedan dañarlos
F	
Firma digital	Es un conjunto de datos asociados a un mensaje digital que permite garantizar la identidad del firmante y la integridad del mensaje
G	
Gusano	Programa que tiene como característica principal la auto replicación con el objeto de colapsar un sistema.
H	
Hacker	Persona que disfruta de ampliar su conocimiento mediante

	la exploración de sistemas programables, buscando siempre ampliar al máximo sus conocimientos.
Hash	Es el resultado de una función o algoritmo para generar claves que representa de manera casi unívoca a un documento, registro, archivo
HIPAA Health Insurance Portability and Accountability Act	Ley de Portabilidad y Responsabilidad del Seguro Médico
I	
IEC International Electrotechnical Commission	Comisión Electrotécnica Internacional
IFAI	Instituto Federal de Acceso a la Información Pública
Información	El conjunto de datos, previamente analizados, razón por la cual adquieren valor.
Ingeniería social	Es la técnica especializada o empírica del uso de acciones estudiadas o habilidosas que permiten manipular a las personas para que voluntariamente realicen actos que normalmente no harían
ISO International Organization for Standardization	Organización Internacional para la Estandarización
K	
Key logger	Es una herramienta utilizada en el desarrollo de software que registra las pulsaciones realizadas en el teclado para almacenarlas en un archivo y enviarlas a través de Internet.
L	
Lammer	Aplicado a aquellas personas que producto de una falta de madurez, sociabilidad o habilidades técnicas, hace que se le considere incompetente en una cierta materia o actividad específica o dentro de un grupo o comunidad.

M	
Malware	Software cuyo objetivo es infiltrarse en un sistema y causar daño en una computadora sin el conocimiento de su dueño
MIT Massachusetts Institute of Technology	Instituto Tecnológico de Massachusetts
N	
NSA National Security Agency	Agencia de Seguridad Nacional de los Estados Unidos
NCC National Computing Centre	Centro Nacional de Computación
Newbie	El empleo de esta palabra se ha extendido para indicar a un recién llegado a cualquier grupo específico.
NOM	Norma Oficial Mexicana.
O	
Outsourcing	Proceso económico en el cual una empresa determinada mueve o destina los recursos orientados a cumplir ciertas tareas, a una empresa externa, por medio de un contrato.
P	
Perfil de protección	Está formado por un conjunto de requerimientos de seguridad los cuales pueden ser los establecidos en los Criterios Comunes o indicados de forma explícita.
Phreaker	Personas que investigan y estudian el funcionamiento de los sistemas telefónicos mediante el uso de tecnología por el placer de manipular un sistema tecnológicamente complejo y en ciertas ocasiones también para poder obtener algún tipo de beneficio como llamadas gratuitas.
Phishing	Anzuelo o estafa electrónica que consiste en implementar técnicas de ingenieria social para adquirir información confidencial mediante la suplantación de sitios de confianza.

Plan de contingencia correctivo	Consiste en el conjunto de procedimientos alternativos al orden normal de una organización, cuyo objetivo es permitir el buen funcionamiento de ésta, una vez que ha sido afectada por algun incidente interno o externo.
Plan de contingencia preventivo	Consiste en el conjunto de procedimientos alternativos al orden normal una organización, cuyo objetivo es permitir el buen funcionamiento de ésta, considerando todos aquellos sucesos tanto internos como externos que puedan afectar la continuidad del negocio.
R	
Riesgo	Posibilidad de ocurrencia de que una amenaza se materialice.
S	
SCFI	Se escriben esas siglas o las del organismo que se encarga de realizar la norma, comúnmente es SCFI.
Scriptkiddie	Se refiere a un cracker inexperto que usa programas, scripts, exploits, troyanos, nukes, que son creados por otros, con la finalidad de romper la seguridad de un sistema.
Seguridad	Conjunto de medidas implementadas para la protección de un bien que posee valor de posibles daños o pérdidas que pueda.
Seguridad de la información	Se encarga del estudio de las medidas implementadas para la prevención y protección de la información, de daños como la modificación, el robo, la revelación al personal no autorizado y la destrucción.
Seguridad de la red	Protección de información, recursos y servicios, realizados por la red de posibles amenazas que puedan afectarlos.
Seguridad informática	Conjunto de herramientas para proteger los sistemas informáticos de amenazas contra la confidencialidad, la integridad y la disponibilidad.
SGSI	Sistema de Gestión de Seguridad de la Información, ISMS es

	el concepto equivalente en idioma inglés, siglas de *Information Security Management System*. Es el concepto central sobre el que se construye ISO 27001, su objetivo es garantizar que la seguridad de la información es gestionada correctamente, mediante un proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo empresarial. Este proceso es el que constituye un SGSI.
Sistema de Identificación Anonimizado	Es el sistema propuesto para que las compañías aseguradoras almacenen el acervo de información cifrada que permita el intercambio seguro entre entidades que estén en otros estados o países.
Sniffer	Programa que tiene por objetivo la captura de tramas en una red.
Spammer	Personas, que se dedica a la distribución o presentación de spam (correo o mensajes considerados basura).
T	
Tarjeta RFID Radio Frequency IDentification	Identificación por radiofrecuencia, es un sistema de almacenamiento y recuperación de datos remotos que usa dispositivos denominados etiquetas, transpondedores o tags RFID. El propósito fundamental de la tecnología RFID es transmitir la identidad de un objeto (similar a un número de serie único) mediante ondas de radio.
Trashing	Personas que obtienen información por medio de la búsqueda en los basureros con el objeto de encontrar información que pudiera resultar importante.
V	
Virus	Es un archivo ejecutable con la capacidad de realizar acciones que no requieran el consentimiento del usuario, con el objeto de comprometer la seguridad de un sistema informático.
VPN	Red Privada Virtual.

Virtual Private Network	Es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet
Vulnerabilidad	Es toda aquella situación que pueda tener como consecuencia un problema de seguridad.

REFERENCIAS

CONTENIDO

BIBLIOGRAFÍA

- ✓ DALTABUIT GODAS, Enrique, *La seguridad de la información*. Limusa, México 2007.
- ✓ HERNÁNDEZ DELGADO, Vicente, *Artículo: Referentes legales para un marco protector de datos personales en México.*
- ✓ G. ALEXANDER, Alberto , *Diseño y Gestión de un Sistema de Seguridad de Información*, Alfaomega Colombiana S.A., Bogotá, D.C., 2007.
- ✓ LOPEZ BARRIENTOS, Jaquelina, QUEZADA REYES, Cintia. *Apuntes de Seguridad Informática*. México, Facultad de Ingeniería UNAM, 2005.

REFERENCIAS ELECTRÓNICAS (Última revisión: 01/05/09)

- ✓ *A Chronology of Data Breaches*
  - http://www.privacyrights.org/ar/ChronDataBreaches.htm
- ✓ *Apuntes Seguridad informática*
  - http://www.lpsi.eui.upm.es/SInformatica/SInformatica.htm
- ✓ *Ataques de tipo DOS y DDOS*
  - http://gabriel.verdejo.alvarez.googlepages.com/DEA-es-2DOS-DDOS.pdf
- ✓ *Cómo elaborar tesis*
  - http://www.tesisimpresa.com.mx/OWL/browse.php?sess=0&parent=66&expand=1&fileid=212
- ✓ *Cómo se hace una tesis*
  - http://www.tesisimpresa.com.mx/OWL/browse.php?sess=0&parent=66&expand=1&fileid=213
- ✓ *Cómo formar una contraseña secreta.*
  - http://www.kreativex.com/blog/?cat=16
- ✓ *Ciclo PDCA*
  - http://es.wikipedia.org/wiki/Deming

✓ *Compliance and Privacy*
- http://complianceandprivacy.com/privacy-laws-and-business/Issue-57.html

✓ *Criptografía y sistema de cifrado*
- http://webdiis.unizar.es/~ftricas/Asignaturas/seguridadD/Transparencias/criptografiaElviraMayordomo.pdf
- http://www.matem.unam.mx/~rajsbaum/cursos/web/presentacion_seguridad_1.pdf
- http://documentacion.redabogacia.org/docushare/dsweb/Get/Document-9895/Criptografia+Basica.pdf
- http://www.iec.csic.es/gonzalo/descargas/AplicacionesCriptografiaEFS.pdf
- http://di002.edv.uniovi.es/~cobas/sr/trans1.pdf
- http://tec.upc.es/sda/Fundamentos%20Criptografia.pdf

✓ *Definición código malicioso*
- http://www.alegsa.com.ar/Dic/codigo%20malicioso.php

✓ *Definición virus*
- http://www.microsoft.com/latam/athome/security/viruses/intro_viruses_what.mspx
- http://seguridad.internet2.ulsa.mx/files/virinfo011.pdf

✓ *Definiciones ejecutores de amenazas de tipo humanas*
- http://es.wikipedia.org/wiki/Phreaker
- http://es.wikipedia.org/wiki/Newbie
- http://es.wikipedia.org/wiki/Script_kiddie
- http://es.wikipedia.org/wiki/Spammer
- http://es.wikipedia.org/wiki/Lammer
- http://es.wikipedia.org/wiki/Hacker

✓ *Definiciones key logger, phishing, sniffer y bomba lógica.*
- http://es.wikipedia.org/wiki/Keylogger
- http://es.wikipedia.org/wiki/Carding
- http://es.wikipedia.org/wiki/Sniffer
- http://es.wikipedia.org/wiki/Bomba_l%C3%B3gica

✓ *Datos personales IFAI-UNAM*
- http://www.ifai.org.mx/SitiosInteres/datosPersonales
- http://www.ifai.org.mx/descargar.php?r=/pdf/ciudadanos/cumplimiento_normativo/&a=Recomendaciones_SDP.pdf
- http://www.enterate.unam.mx/Articulos/2003/octubre/protecci.htm

- www.davara.com
- http://www.ifai.org.mx/SitiosInteres/leyesInternacionales

✓ *Estándares serie 27000*
- http://es.wikipedia.org/wiki/ISO/IEC_27000-series
- http://www.iso27000.es/download/doc_iso27000_all.pdf
- http://www.revista-ays.com/DocsNum25/Normas/Suarez.pdf

✓ *El derecho a la protección de datos personales en México*
- http://www.madrid.org/comun/datospersonales/0,3126,457237_0_127535941_12490604_12489303,00.html

✓ *Frases celebres relacionadas con la seguridad de la información.*
- http://seguridad-informacion.blogspot.com/2007/09/algunas-citas-famosas-relacionadas-con.html
- http://new.taringa.net/posts/info/1206004/101-citas-c%C3%A9lebres-del-mundo-de-la-inform%C3%A1tica.html

✓ *Freedom security and justice*
- http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm
- http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm

✓ *HIPAA*

- http://www.tricare.mil/mybenefit/espanol/ProfileFilter.do;jsessionid=Kj2T9pnmYdLSVXJnnbyHXcvdh0QPchQpkyQ3znvmJLQLpdm4qMJn!217405207?puri=%2Fhome%2FMedical%2FRecordsAndPrivacy%2FHIPPAPrivacy

✓ *Información aseguradoras*
- http://www.eeconomia.gob.mx/wb2/eMex/eMex_Que_sabes_sobre_los_agentes_de_seguros
- http://es.wikipedia.org/wiki/RFID

✓ *Iniciativa de Ley Federal de Protección de Datos Personales*
- http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf

✓ *Information Security Handbook: A Guide for Managers*
- https://www.agpd.es/portalweb/canaldocumentacion/legislacion/iberoamerica/proyectos/common/pdfs/Iniciativa-de-Ley-Federal-de-Proteccin-de-Datos-Personales--ap-original-cp-.pdf

- ✓ *Ley Federal del Derecho de Autor*
  - http://www.edicion.unam.mx/pdf/LFDAUTOR.pdf

- ✓ *Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental*
  - http://www.ifai.org.mx/transparencia/LFTAIPG.pdf

- ✓ *Ley de Instituciones de Crédito*
  - http://www.cddhcu.gob.mx/LeyesBiblio/pdf/43.pdf

- ✓ *Ley para Regular las Sociedades de Información Crediticia*
  - http://www.cgeson.gob.mx/SERVICIOS/LEYES/federales/leyes/Ley_Regula_Soc_Information.pdf

- ✓ *Ley de Protección de Datos Personales para el Distrito Federal*
  - http://www.sederec.df.gob.mx/mjuridico/pdf/datosPersonales.pdf

- ✓ *Libro seguridad en UNIX y redes*
  - http://www.rediris.es/cert/doc/unixsec/unixsec.pdf

- ✓ *Manual para la elaboración de una tesis de doctorado.*
  - http://www.tesisimpresa.com.mx/OWL/browse.php?sess=0&parent=66&expand=1&fileid=214

- ✓ *Métodos de cifrado simétrico y asimétrico*
  - http://www.alfa-redi.org/rdi-articulo.shtml?x=282
  - http://www.darkineses.com/reportajes/criptografia.php
  - http://es.kioskea.net/contents/crypto/crypto.php3
  - http://es.wikipedia.org/wiki/Hash
  - http://www.dirinfo.unsl.edu.ar/~seguridadred/teorias/clase5.pdf
  - http://www.cripto.es/expedien/exped005.htm
  - http://es.wikipedia.org/wiki/Claves_RSA
  - http://www.ing.ula.ve/~ibc/ayda/c26rsa.pdf
  - http://es.wikipedia.org/wiki/Diffie-Hellman
  - http://materias.fi.uba.ar/6669/docs/Diffie-Hellman.pdf
  - http://www.sociedaddesarrollo.com/webnueva/noticias/editor/pag/download.php3?idfichero=119

- ✓ *OECD Privacy Statement Generator*
  - http://www.oecd.org/document/39/0,3343,en_2649_34255_28863271_1_1_1_1,00.html

- ✓ *Protecting personal information a Guide for Business*
  - www.ftc.gov/bcp/edu/pubs/business/privacy/bus69.pdf

- ✓ *Protección de datos personales en México: el caso del poder ejecutivo federal*
  - http://www.bibliojuridica.org/libros/libro.htm?l=2299

- ✓ *Plan de contingencia preventivo y correctivo*
  - http://www.forodeseguridad.com/artic/segcorp/7209.htm

- ✓ *Recomendaciones de seguridad*
  - http://www.rediris.es/cert/doc/docu_rediris/recomendaciones/recomendaciones.pdf

- ✓ *Recomendaciones de seguridad de datos personales*
  - http://www.ifai.org.mx/descargar.php?r=/pdf/ciudadanos/cumplimiento_normativo/&a=Recomendaciones_SDP.pdf

- ✓ *Red privada virtual (VPN)*
  - http://es.wikipedia.org/wiki/Red_privada_virtual

- ✓ *Respaldos de información*
  - http://www.ehu.es/scwreall/ehu/backups/plan-backups.html
  - http://www.perantivirus.com/sosvirus/pregunta/ingsocial.htm

- ✓ *Servicios de seguridad de la información.*
  - http://www.iec.csic.es/criptonomicon/seguridad/servicio.html

- ✓ *Tesis Seguridad de la Información*
  - http://www.segu-info.com.ar/tesis/

IMÁGENES

REFERENCIAS ELECTRÓNICAS (Última revisión: 01/05/09)

- http://genesis.uag.mx/posgrado/revistaelect/images/hackers2.gif
- http://www.jomagaro.es/wp-content/uploads/2007/09/seguridad.png
- http://www.munoz.com.py/images/img_links.jpg
- http://www.ingecomp.us/DSL_Redes_Computadoras/DSL_Re7.gif
- http://www.subirimagen.net/images/110387USB1.JPG
- http://www.educared.cl/images/general_chile/cd.jpg
- http://www.elrancahuaso.cl/tmp_images/108/noticia_5375_normal.jpg
- http://seguridadinformaticajvg.nireblog.com/post/2007/11/20/seguridad-informatica
- http://upload.wikimedia.org/wikipedia/commons/f/f9/Cifrado_por_bloques.png
- http://www.cucurrucu.com/analisis-del-texto-tendencias-en-educacion-en-la-sociedad-de-las-tecnologias-de-la-informacion/
- http://pics.miarroba.com/users/m_nophoto.jpg
- http://www.userinterfaceicons.com/preview.php
- http://www.backtoessentials.com/graphics/120-free-icon-sets-to-enhance-user-interfaces/
- http://www.eoimurcia.org/se_procedimiento.htm
- http://www.revista.unam.mx/vol.9/num4/art20/art20.pdf
- http://www.flickr.com/photos/ingeantonio/2507099843/
- http://tecresource.com/page10.html
- http://downloads.ziddu.com/downloadfiles/914072/ICONKI.rar
- http://www.chasquinet.org/alertc/images/stories/Image/incendio%20edificio.jpg
- http://www.noesficcion.com/wp-content/ladron-copia.jpg
- http://www.nngov.com/library/images/book3
- http://www.iconarchive.com/show/dragon-soft-icons-by-artua/User-icon.html

- ✓ http://2.bp.blogspot.com/_TJMCIy6tFaE/SSZs3l6faYI/AAAAAAAAALw/10cdZdRgCRA/s320/DoS.jpg
- ✓ http://es.wikipedia.org/wiki/C%C3%B3digo_maligno