UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES ARAGÓN

ANÁLISIS DE RIESGOS EN LA SEGURIDAD INFORMÁTICA

TRABAJO ESCRITO BAJO LA MODALIDAD DE SEMINARIOS Y CURSOS DE ACTUALIZACIÓN Y CAPACITACIÓN PROFESIONAL

QUE PARA OBTENER EL TÍTULO DE:

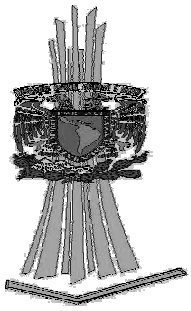
INGENIERO EN COMPUTACIÓN

P R E S E N T A:

DANIEL SAAVEDRA FLORES

ASESOR:

M. en C. LEOBARDO HERNÁNDEZ AUDELO



SAN JUAN DE ARAGÓN, EDO. DE MÉXICO, 2010.

Dedicatorias

Este trabajo se los dedico a quienes con su dedicación y cariño me han apoyado en las diferentes etapas de mi vida.

Con respeto y gratitud a mis padres por que siempre han estado ahí con su apoyo y consejo:

María de los Ángeles Flores Montiel
Gregorio Saavedra Picazo

Con cariño a mis hermanos:

Isabel Saavedra Flores
Israel Saavedra Flores

A mi abuela:

Oliva Montiel Flores

A mis amigos con los que he recorrido muchos años de mi vida, además del placer de conocerlos:

Alfonso Rodrigo Ramírez Rosas
Alfredo Anduaga Ramírez
Juan Carlos Camacho Alvarez

Agradecimientos

A la máxima casa de Estudios, la UNAM, y en particular a la Facultad de Estudios Superiores Aragón, porque en sus aulas tuvimos la fortuna de adquirir conocimiento Universal y por los gratos momentos pasados en ellas.

Al M. en C. Leobardo Hernández Audelo mi gratitud por la dirección del presente trabajo.

Al M. en C. Marcelo Pérez Medel por el apoyo que me ha brindado todo este tiempo.

A los profesores de la carrera de Ingeniería en Computación, ya que ellos compartieron sus conocimientos y nos brindaron su apoyo cuando lo llegamos a necesitar.

A todos mis amigos a los cuales conocí durante mi estancia en la Universidad, pues con ellos compartí muchos momentos agradables a lo largo de varios años.

A mis ex compañeros de trabajo, de los cuales aprendí muchas cosas y estuvieron siempre dispuestos a ayudarme en cualquier situación en la que me encontrase.

Índice

Índice de Tablas

Índice de Figuras

Convenciones

Se utilizaron a lo largo de este trabajo las siguientes convenciones:

1. Anglicismos: en letras itálicas o cursivas como se muestra a continuación: *(“Information Security”)*

2. Palabras clave: se encuentran en negritas. Por ejemplo: **Salvaguarda**

3. Citas: se encuentran utilizando el texto de la cita entrecomillado y en letras itálicas como se muestra a continuación: *“La Seguridad Informática es…”*

4. Títulos de Tablas y Figuras: Se encuentran en letra Times New Roman pt 11 centrados y en negritas justo debajo de la figura

5. Hipervínculos: Se encuentran subrayados, por ejemplo: http://es.wikipedia.org

Títulos y Subtítulos

Los siguientes tamaños de letra se refieren los títulos y subtítulos (como puede observarse en la estructura del índice).

Formato	Descripción
Título Capítulo	Utilizado para el título del capítulo ARIAL Black 20 pt
1Título	Utilizado para Títulos en primer nivel ARIAL 18 pt Negritas
1.1Título	Utilizado para subtítulos en segundo nivel ARIAL 16 pt Negritas
1.1.1Título	Utilizado para subtítulos en tercer nivel ARIAL 14 pt Negritas
1.1.1.1Título	Utilizado para subtítulos en cuarto nivel ARIAL 12 pt Negritas
1.1.1.1.1Título	Utilizado para subtítulos en quinto nivel Times New Roman 13 pt Negritas
Texto en general	Utilizado para el desarrollo de temas y subtemas ARIAL 12 pt Normal

Bibliografía:

Las referencias tomadas de libros o páginas web se indicarán usando números arábigos con paréntesis cuadrado al final del texto, por ejemplo:

…debido a las políticas de seguridad [3].

Posteriormente, en la Bibliografía con el número indicado se podrán consultar los datos del libro consultado donde:

- El Autor u organismo emisor está con letras itálicas ARIAL 10 pt.
- El nombre del libro está entrecomillado y en negritas con letras ARIAL 10 pt.

Por ejemplo:

Rolf Oppliger **"Contemporary Cryptography"** Ed. Artech House. Primera Edición. Publicado en Estados Unidos en el año 2005
.

Prólogo

En los últimos años el hombre ha empezado a depender en gran medida de las Tecnologías de Información (TI), las cuales han tenido una evolución muy acelerada y continuarán evolucionando de una manera un tanto incierta. Como resultado de esta evolución, muchas de las actividades realizadas en la vida diaria de las personas tienden a apoyarse en las TI, esto crea una dependencia que no había existido antes. Las actividades que hoy se basan en TI se realizaban desde mucho tiempo antes de la aparición de estas nuevas tecnologías, es decir, los bancos realizaban sus actividades bancarias desde antes de que existieran las computadoras, no obstante, la diferencia con la actualidad es que por las ventajas y comodidades que ofrece la tecnología actual se dejaron de usar las técnicas antiguas, de tal forma que actualmente es impensable volver a operar como se hacía hace 10 o 20 años.

Una de las tecnologías más recientes y que tiene un impacto importante en nuestras actividades diarias es Internet. Internet es una tecnología que actualmente permite realizar distintas actividades de forma más rápida y sencilla. Por ejemplo, con el correo electrónico es posible comunicarse con diferentes personas en distintas partes del mundo en poco tiempo, algo que con el correo convencional tomaría días o incluso semanas. El servicio de banca electrónica permite realizar actividades tales como el servicio de los bancos para actividades tales como compras a través de Internet, realizar diferentes tipos de pagos, abonar crédito a un teléfono celular, e incluso realizar transferencias de dinero a otras cuentas bancarias.

A nivel de empresa Internet es un medio que ayuda a mantener la comunicación de los dueños y empleados de la empresa con clientes, proveedores, socios y distintas personas, lo cual facilita a la empresa poder ofrecer servicios a través de los cuales obtendrá ganancias, prestigio y un lugar en el mercado actual.

Todas estas nuevas tecnologías han significado cambios en la forma de realizar las actividades de las empresas y de las personas, y sin embargo, como en todo, existen riesgos al usar tecnologías recientes. Tanto las computadoras como Internet, así como diferentes aplicaciones, fueron diseñados desde un principio para ser fáciles de utilizar, pero estas tecnologías no fueron diseñadas para ser seguras en su uso, lo cual origina diferentes escenarios que pueden llegar a parecer historias de ficción. Es muy común escuchar de fraudes electrónicos, o que si salió una nueva versión de un virus dañino, o diferentes noticias donde la seguridad de las computadoras o de la red interna de alguna institución fueron violadas; muchos de estos sucesos se deben a que las computadoras, Internet y las aplicaciones no tomaron en cuenta aspectos de seguridad desde un principio, lo lamentable de todo esto es que se ha llegado a un punto en el que no se pueden volver a rediseñar las computadoras, así como tampoco se puede volver a crear Internet o muchas de las aplicaciones que usamos todos los días para que sean seguras. Hay que entender que es necesario trabajar con lo que se tiene, corrigiendo los errores que existen y buscar alternativas para poder garantizar cierto

nivel de seguridad y así mismo desarrollar estrategias que permitan un funcionamiento de la empresa donde haya un equilibrio entre la seguridad y la operatividad de la empresa.

Actualmente la seguridad es vista como un mal necesario ya que darle seguridad a un sistema es caro, representa cierta dificultad y no tiene un retorno de inversión tangible, es decir, no hay un beneficio económico claro en la seguridad de la información, lo cual origina que los dueños de las empresas no vean necesario tomar medidas para evitar diferentes amenazas hasta que ocurre un evento que afecta la seguridad y origina pérdidas para la empresa.

Ya sea porque se afecto la seguridad de la información de la empresa o por que se cobra conciencia de proteger tanto a las tecnologías como a la información, es importante saber por dónde hay que continuar. El primer paso siempre será darse cuenta de que existe un problema que hay que solucionar.

Actualmente la forma de corregir los problemas de la Seguridad Informática se basa en el uso de herramientas las cuales en sus especificaciones dicen que pueden resolver diferentes tipos de problemas, otra forma de solucionar los problemas de seguridad es acudir a diferentes empresas que se dedican a dar soluciones de seguridad cuyos costos son elevados, lo cual hace que sea poco viable para la mayoría de las empresas.

Sería un error empezar a gastar recursos antes de saber qué es lo que realmente necesita la empresa, no se pueden empezar a solucionar los problemas de seguridad si antes no se estudia qué es lo que se tiene que solucionar. Si se empiezan a buscar herramientas, cada proveedor va a asegurar que los problemas de las empresas se resuelven comprando las soluciones que ellos ofrecen. Independientemente de si la solución ofrecida realiza correctamente su trabajo, no es seguro que funcione para una determinada empresa si ésta no la necesita.

Entonces pues, la solución para evitar gastar el dinero en soluciones que no necesariamente servirán para una empresa es identificar las vulnerabilidades, amenazas y riesgos que tiene la empresa. Tener el conocimiento de los eventos que pudieran afectar a la empresa es lo que dará la pauta para saber hacia dónde dirigir los recursos, qué tipo de herramientas pueden funcionar y qué servicios y mecanismos de seguridad son los que realmente se necesitan.

Debido a la importancia que tiene el Análisis de Riesgos es que se realizó el presente trabajo, el cual tiene por objetivo dar a conocer el concepto del Análisis de Riesgos, mostrar donde es que se encuentra dentro de la Seguridad Informática, describir con que conceptos es que se relaciona y dar a conocer algunas de las metodologías con las cuales es posible llevarlo a cabo. El contenido de este trabajo está contenido en 6 capítulos cuyo contenido se describe a continuación:

En el **Capítulo 1** se explica lo que es la seguridad de la información, se da una introducción a la seguridad, se explica su importancia, se mencionan los diferentes

servicios y mecanismos que forman parte de la Seguridad Informática y se da una breve introducción a la Criptografía.

En el **Capítulo 2** se explica primero el Ciclo de Vida de la Información y a continuación el proceso dinámico de la Seguridad Informática, se identifican sus procesos y se ubica donde es que se lleva a cabo el Análisis de Riesgos.

En el **Capítulo 3** se mencionan diferentes estándares y controles que actualmente se usan como lineamientos para garantizar cierto nivel de seguridad para las empresas y los procesos.

En el **Capítulo 4** se trata a cerca del Análisis de Riesgos, se explica en qué consiste, que etapas involucra y por qué es importante para poder ofrecer Seguridad Informática a las empresas.

En el **Capítulo 5** se da una explicación de diferentes metodologías para realizar el Análisis de Riesgos, donde se explica de manera general cuales son los pasos que siguen, y al final se hace un análisis comparativo donde se resaltan las ventajas y desventajas que existen en cada metodología.

En el **Capítulo 6** se explican los resultados a los que se llego en este trabajo junto con las conclusiones a las cuales se obtuvieron a partir de haber estudiado las diferentes metodologías para el Análisis de Riesgos.

Capítulo

1

Seguridad Informática

Resumen

Desde tiempos muy antiguos la información ha sido muy importante para la toma de decisiones de las personas, en base a la información es que se pueden tomar diferentes decisiones, sin embargo, hablar de la información no es un tema sencillo, ya que ésta se encuentra en diferentes estados y puede usarse de distintas formas.

La información desde tiempos remotos ha tenido problemas de seguridad, emperadores, reyes o gobernantes que han estado en conflicto con otros gobernantes han ganado ventaja cuando obtienen conocimiento de información secreta de los demás gobernantes, es por ello que desde aquellas épocas se protegía la información. En la actualidad con el uso de las tecnologías de información, se repiten algunas de las situaciones que existían anteriormente sin embargo también se suman nuevas amenazas y nuevos riesgos que son inherentes a las nuevas tecnologías.

Actualmente la información ya no sólo se encuentra en medios impresos como libros, papeles o escritos, hoy en día la información puede encontrarse en medios electrónicos muy diversos. La información puede almacenarse en servidores, computadoras de escritorio, computadoras portátiles (laptops), memorias USB ó incluso en teléfonos celulares así como en otros medios portables; estos últimos medios pueden llegar a suponer un gran peligro para las empresas, ya que por su tamaño y capacidad se pueden utilizar fácilmente para extraer información de una empresa sin que puedan ser detectados. Y si hablamos de los teléfonos celulares que se usan actualmente, el problema no se queda en que puedan almacenar información, debido a las nuevas características que éstos incorporan pueden tomar fotos con una nitidez aceptable, pueden grabar conversaciones, videos e incluso enviar pequeños mensajes de texto a otros teléfonos celulares.

Estos ejemplos hacen ver que en realidad proteger la información es una tarea cada vez más compleja, pero al mismo tiempo necesaria.

---

1 Seguridad Informática

1.1 Seguridad de la Información

La Seguridad Informática o Seguridad de la Información, es el conjunto de políticas y mecanismos que permiten preservar la Confidencialidad, Integridad y la Disponibilidad de los recursos de un sistema. Los principales servicios de seguridad son los que conforman el Triangulo CIA, el cual obtiene su nombre por sus siglas en inglés: *Confidenciality, Integrity* y *Availability* [1].

1.2 Importancia de la Seguridad de la Información

Es importante proteger la información de la empresa ya que el mercado es cada vez más competitivo y la información puede llegar a hacer una gran diferencia entre obtener el éxito o fallar en cumplir con los objetivos de la empresa.

La finalidad de la Seguridad Informática es proteger la información de un gran número de amenazas para garantizar la continuidad del negocio, minimizar los riesgos de la empresa, maximizar el retorno en la inversión y aprovechar las oportunidades de negocio.

La información de una empresa es un activo, el cual como los demás activos de la empresa tiene un valor para la organización y es por ello que se debe proteger [1]. Debido a esto es necesario convencerse de la importancia de proteger la información de la empresa ya que la información está expuesta a diferentes amenazas de las cuales incluso se puede llegar a ignorar su existencia.

Actualmente se empieza a depender en gran medida de las Tecnologías de Información y es importante resaltar que la mayoría de los sistemas de información no han sido diseñados para ser seguros, por ejemplo cuando se diseñó la comunicación entre redes lo que se buscaba era poder hacer rápida y fácil la comunicación, nunca se consideraron los problemas de seguridad que esto podría ocasionar.

Algo preocupante para las empresas es que actualmente en Internet existe una gran cantidad de programas y aplicaciones disponibles que afectan los servicios de seguridad y los estados de la información, y cualquier persona puede bajar esas aplicaciones y usarlas. Algunas herramientas son sencillas de usar y no requieren conocimientos muy amplios para su utilización, también existen otras herramientas que no son tan sencillas de utilizar; sin embargo, existe también un buen número de manuales e incluso videos que explican paso a paso como poder realizar diferentes acciones con dichas herramientas. Esta situación ha hecho que en los últimos años se haya incrementado el número de amenazas en la red.

Ejemplos de incidentes de seguridad hay muchos y en ocasiones pudieran llegar a parecer historias sacadas de películas de ciencia ficción.

Tenemos por ejemplo a Jonathan James, un adolescente de 16 años que fue sentenciado a 6 meses de arresto domiciliario. Entre sus acciones más destacables se encuentra una intrusión a la Agencia de Reducción de Amenazas de la Defensa en los Estados Unidos, dicha agencia se encarga de reducir las amenazas a los Estados Unidos y a sus aliados de armas nucleares, químicas y biológicas, entre otras. Jonathan James instaló un *backdoor* en un servidor de esta agencia con el cual logro ver correos electrónicos de asuntos sensitivos y obtener nombres de usuario y contraseñas de los empleados. Otro ataque realizado por este mismo personaje fue el robo de software de la *National Aeronautics and Space Administration* (NASA) por un valor aproximado de 1.7 millones de dólares. Entre el software robado estaba un programa utilizado para

controlar la temperatura y humedad de la Estación Espacial Internacional. La NASA paró por 21 días el uso de sus computadoras ocasionando pérdidas por 41,000 dólares [2].

Otro caso muy conocido en el año 2000 fue el virus *"I love you"*, este virus se propagaba a través del correo electrónico, llegaba con el texto **ILOVEYOU** como asunto y venía con un archivo adjunto llamado "**LOVE-LETTER-FOR-YOU.TXT.vbs**". En el momento en que los usuarios abrían el correo, automáticamente el virus se enviaba a sí mismo a toda la lista de contactos de la víctima, logrando de esta manera expandirse rápidamente. El virus comenzó a propagarse el 4 de mayo del año 2000 en Filipinas y en un solo día recorrió gran parte del mundo infectando al 10% de las computadoras conectadas a Internet y causando un daño de 5.5 billones de dólares [3].

A pesar de que existen casos donde los atacantes usaron su intelecto para poder cometer un ataque, actualmente la facilidad del uso de herramientas para alterar los sistemas y su accesibilidad a ellas a través de la red ha originado que personas con no muchos conocimientos logren ser una amenaza. Un ejemplo de esto lo tenemos con Jan de Wit, este personaje fue el autor del virus **Kournikova**. La particularidad de este virus es que a pesar de haberse propagado por la red y ser motivo de alarma para muchos, el virus fue creado por medio de un programa llamado **VBS Worm Generator**, dicho programa se puede descargar en Internet, el cual por si fuera poco cuenta con un ambiente gráfico donde se pueden seleccionar las características que se desea que tenga el virus [4].

Estos escenarios realmente pueden parecer verdaderas historias de terror para los dueños de diferentes empresas que tienen que proteger sus activos y su información, no obstante es importante tener conocimiento acerca de la empresa, de lo que se desea realmente proteger e identificar y que servicios de seguridad son realmente necesarios.

1.3 Servicios de Seguridad

La seguridad de la información se protegerá dependiendo de qué servicios de seguridad se deseen preservar en los activos de la empresa. Los servicios de seguridad vienen siendo las características deseadas de seguridad de la información cuando ésta se encuentra en diferentes estados, los cuales se describen en el Capítulo 2.

A continuación se describen los servicios de seguridad que ofrece el Triángulo CIA mencionados en este capítulo anteriormente.

Confidencialidad implica que los datos transmitidos, ya sea a través de una computadora, una red, o algún otro medio, sean revelados sólo a personas autorizadas [5]. Este servicio puede no sólo incluir el hecho de proteger el conocimiento de los datos de personas no autorizadas, sino incluso el hecho de llegar a saber que la información existe. Algunos datos son valiosos porque no son muy conocidos. Por ejemplo, para una compañía farmacéutica, una fórmula de un medicamento es algo que le toma tiempo y le cuesta recursos desarrollarla, si dicha compañía invierte en la fabricación de

sus fórmulas es para tener una ventaja competitiva en el mercado y así obtener ganancias. La sensibilidad de la información hace necesario que sean protegidos los datos y los equipos que la contienen, los equipos deben de ser protegidos contra ataques, usos no autorizados y otros sucesos que pueden llevar a la revelación imprevista de datos confidenciales.

Una ruptura en el servicio de confidencialidad se da cuando la información es revelada, ya sea de manera intencional o accidental, a personas no autorizadas.

Integridad es el grado en que se puede confiar que los datos estén completos y sean exactos; esto es, el grado de confianza en que los datos no han sido modificados incorrectamente ya sea por malicia, negligencia o por accidente [6]. Este servicio de seguridad es importante, ya que si un dato deja de ser exacto pierde su valor y por lo tanto no se podrá confiar en él, incluso si la información se corrompe totalmente, el valor de los datos se pierde completamente. Los sistemas de información deben de ser protegidos frente a sucesos que puedan provocar la modificación no autorizada de los datos.

Disponibilidad implica que los usuarios puedan acceder a la información en el momento en que lo requieran o en ciertos períodos de tiempo ya preestablecidos. Este concepto está también asociado en el concepto de **Denegación de Servicio** [7]. Por ejemplo, Amazon.com es una página que se dedica al comercio electrónico, esta empresa como muchas otras han sido víctimas de ataques de Denegación de Servicio los cuales tienen la finalidad de evitar que los posibles clientes puedan acceder a las páginas de los vendedores. No es difícil imaginar que si un negocio que depende de las ventas por el comercio electrónico no puede dar a conocer sus productos o servicios a través de Internet, sufrirá pérdidas que podrían llegar incluso a poner en riesgo la existencia de la empresa.

Aunque los servicios que incluye el Triángulo CIA son importantes, muchos autores añaden otros servicios como **Autenticación**, **No repudio** y **Control de acceso**, los cuales se describen a continuación:

La **Autenticación** es el proceso de verificar que la identidad de las partes involucradas en alguna operación es válida, en otras palabras, es confirmar a algo o a alguien como auténtico [7]. Para llevar a cabo la autenticación, es necesario que de la persona a la que se va a autenticar se conozca información adicional con la cual poder validar su identidad. Normalmente la comprobación de la identidad de un sujeto se realiza en base a uno o más factores los cuales se encuentran en una base de datos que contiene identidades válidas. La autenticación se puede confirmar con algo que se sabe, con algo que se tiene, o con algo que se es. Algo que se sabe normalmente se refiere a un password, algo que se tiene puede ser una credencial o un token, en cuanto a algo que se es se refiere al uso de autenticadores biométricos; los autenticadores biométricos se basan en la medición de algún rasgo de una persona, el rasgo puede ser la huella dactilar, la forma del iris, el rostro, etc.

El servicio de **No repudio** se asegura de que una persona que está involucrada en algún evento no pueda negar que el evento ocurrió. Sirve para prevenir que un sujeto niegue haber mandado un mensaje, que diga que no llevó a cabo alguna acción o incluso que niegue haber sido la causa de algún evento [7].

El servicio de **Control de Acceso** determina a que información puede llegar a acceder un individuo, y dependiendo de la información a la cual pueda acceder también se determinarán qué operaciones puede realizar con dicha información, ya sea para leer, escribir, ejecutar o incluso borrar [5]. Para su implementación se pueden usar listas de control de acceso o modelos matriciales.

Es importante que cuando se pretenden implementar estos servicios en un sistema, se identifiquen cuáles son los servicios que realmente se necesitan. Por ejemplo, si la información que se va a manejar es pública, no será necesario implementar mecanismos de confidencialidad, otro ejemplo lo tenemos en las páginas cuyas ganancias yacen en las visitas a sus sitios, éstas no se verían para nada beneficiadas si se les implementase el servicio de control de acceso. Se deben identificar cuáles servicios sí se requieren y cuáles no, ya que si algo caracteriza a la Seguridad Informática es que no hay bueno, bonito y barato. Por cualquier servicio que se desee implementar habrá que pagar un precio, ya sea económico (comprando una solución comercial o desarrollada por la misma empresa), de flexibilidad (cuando se hacen más estrictas las políticas de la empresa) o en rendimiento (cuando la solución de seguridad incrementa el tráfico en la red).

Para poder implementar un servicio de seguridad es necesario hacerlo por medio de mecanismos de seguridad, los cuales se describen a continuación.

1.4 Mecanismos de Seguridad

Los servicios de seguridad, como ya se mencionó, son las características de seguridad que se desean en el contexto de la seguridad de la información, no obstante para poder implementarlos, se utilizan los mecanismos de seguridad. Los mecanismos de seguridad son las funcionalidades o técnicas mediante las cuales es posible llevar a cabo los servicios de seguridad. Estos mecanismos están descritos en el ISO 7498-2 [8]. Los mecanismos para implementar los servicios de seguridad se muestran en la Tabla 1.1.

Servicio	Mecanismo(s)
Confidencialidad	Cifrado
Integridad	Cifrado, Firma Digital
Autenticación	Cifrado, Firma Digital, Autenticadores
No Repudio	Firma Digital, Notarización
Control de Acceso	Políticas de Control de Acceso

Tabla 1.1 Servicios y mecanismos de seguridad

En el capítulo 3 se describirán más a detalle los diferentes servicios y mecanismos de seguridad cuando se hable del ISO 7498-2; sin embargo, es necesario señalar que a diferencia del servicio de Control de Acceso, los mecanismos de Confidencialidad, Integridad, Autenticación y No Repudio se basan de algún modo en la **Criptografía**, la cual a su vez es parte de la **Criptología**. Es por ello que la Criptografía tiene gran importancia en la Seguridad Informática, por lo cual a continuación se dará una breve introducción.

1.5 Criptología

El termino Criptología se deriva de las palabras griegas "*kriptos*" que se traduce como oculto y "*logos*" que se traduce como palabra, por lo cual, Criptología se puede entender como "palabra oculta". Esta interpretación se refiere a la intención original de la Criptología, la cual pretendía ocultar el significado de palabras especificas para proteger la confidencialidad de la información, no obstante, en la actualidad el término Criptología se refiere a la ciencia que se encarga de estudiar los criptosistemas en cuanto a sus técnicas de diseño y eficiencia [9], para ello cuenta con dos ramas principales que son la **Criptografía** y el **Criptoanálisis**, aunque dependiendo de las fuentes que se consulten también suele incluirse la **Esteganografía**.

1.5.1 Esteganografía

La Esteganografía proviene de la palabra griega “*stegos”*, que significa ocultar. La Esteganografía es el conjunto de técnicas que permiten ocultar o camuflar cualquier tipo de datos, dentro de información considerada como válida. Para lograr este fin se vale de diferentes técnicas, que son: **Adición** (ocultando el mensaje secreto en las secciones del medio portador que pueden ser ignoradas por la aplicación que lo procesa), **Substitución** (modificando ciertos datos del medio portador por los datos de mensaje secreto) y **Generación** (se crea el esteganograma a partir de la información secreta, sin contar con un medio portador previamente) [10].

Los elementos necesarios para poder ocultar información por medio de la Esteganografía son: **un medio portador** donde se va a ocultar la información, este puede ser un archivo de cualquier tipo, como archivos de imagen, de video, de sonido, software, texto, etc., también será necesario un **algoritmo de esteganografía** para poder ocultar la información, así mismo una **llave de cifrado** para poder ocultar y posteriormente recuperar la información y finalmente la **información a ocultar**.

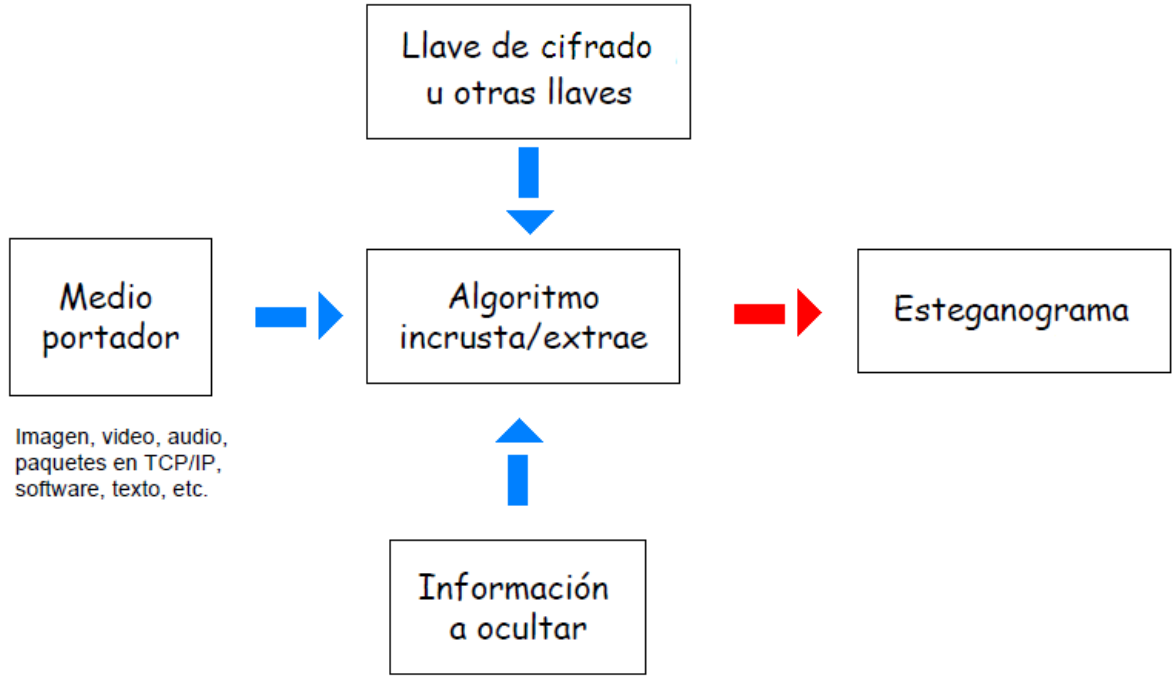


Figura 1.1 Proceso Esteganográfico

La Figura 1.1 describe el proceso para ocultar la información por medio de la Esteganografía.

La principal ventaja que tiene la Esteganografía sobre la Criptografía, es que en la Esteganografía se puede mandar un mensaje oculto, pero dando la apariencia de que lo que se está mandando en realidad es cualquier otro tipo de información.

Es posible combinar el uso de la Criptografía con la Esteganografía, es decir, se puede cifrar un archivo y después ocultarlo en otro archivo mediante la Esteganografía, de esta forma aunque se logre extraer el archivo oculto, éste estará cifrado y de cualquier forma no será entendible por aquellas personas a quienes no va dirigida la información.

1.5.2 Criptografía

La palabra Criptografía viene de las palabras griegas "*krypto"* que significa "oculto" y "*graphos"*, que significa "escribir", consecuentemente criptografía significa "escritura oculta". La criptografía es la ciencia de usar matemáticas para cifrar o descifrar datos con la finalidad de convertir el significado de un texto en algo ininteligible. La criptografía permite almacenar de manera segura información sensitiva o bien transmitirla a través de medios inseguros como lo es Internet, de manera que no pueda ser leída por nadie excepto por personas que deban de tener acceso a dicha información [10].

El cifrado de la información no es algo nuevo, desde hacía ya mucho tiempo se buscaba proteger la información, ya sea que fuese para ocultar secretos de estado o estrategias militares.

La criptografía clásica se basó en las técnicas de ocultamiento, transposición, permutación y substitución. La criptografía clásica se desarrolló para poder ocultar los mensajes militares de los enemigos, estos criptosistemas se basaron en el ocultamiento de la llave y del algoritmo usado. Actualmente eso ha cambiado, la seguridad se basa en la fortaleza del algoritmo y en la complejidad de la llave.

Como se mencionó anteriormente, la criptografía sirve de mecanismo para implementar la mayoría de los servicios de seguridad, sin embargo esto no lo hace de una sola forma, sino que para ello utiliza diferentes técnicas.

Actualmente las técnicas utilizadas en la criptografía son las Funciones Hash, Cifrado Simétrico y el Cifrado Asimétrico, las cuales se describen brevemente a continuación.

1.5.2.1 Funciones Hash

Una función hash, también conocida como función resumen o función digestiva, es una proyección de un conjunto, generalmente con un número elevado de elementos, sobre un conjunto de tamaño fijo y mucho más pequeño que el anterior. Dicho de otra forma, las funciones hash toman como entrada un bloque de datos de longitud variable y lo transforman en un bloque de datos de longitud fija, con la particularidad de que pequeñas modificaciones al bloque de datos de entrada producen una salida completamente distinta, haciendo esto que (en teoría) dos conjuntos de datos distintos generen una salida completamente diferente [11].

Los algoritmos hash más conocidos son:

- MD5 diseñado por Ron Rivest como mejora del MD4. Procesa el texto en bloques de 512 bits y produce 128 bits.

- SHA1, diseñado por NIST y NSA, procesa bloques de 512 bits y produce 160 bits.

- RIPE-MD, diseñado bajo el proyecto europeo RIPE (RACE), también es una variante de MD4 aumentando su seguridad, produce 128 bits.

- HMAC, es una función hash que incluye una clave, sólo alguien con la misma clave puede verificar el hash.

Las funciones hash sirven como mecanismo para verificar la integridad de la información. La salida producida por una función hash aplicada a un documento se conoce como la **Huella Digital** de dicho documento. Cualquier cambio a ese documento

produce una huella digital diferente, es por ello que si se modifica el mensaje original aunque sea por un carácter en el proceso de la transmisión de la información, la huella digital indicará que hubo un cambio durante la transmisión.

En el proceso de autenticación las Funciones Hash se emplean de una forma diferente. Por ejemplo, los sistemas operativos UNIX y Windows en sí no almacenan las contraseñas de los usuarios como texto en claro ya que de ser así cualquiera podría buscar el archivo donde se guardan las contraseñas y obtener de esta manera las contraseñas de los usuarios. Lo que hacen los sistemas operativos es guardar el resultado del hash de la contraseña del usuario, cuando el usuario ingresa su contraseña en un sistema operativo de la contraseña ingresada se obtiene su hash y éste se compara con el hash que se encuentra guardado en el sistema operativo, si el hash obtenido de la contraseña ingresada por el usuario es igual a la almacenada se le dará acceso al sistema, en caso contrario se le negara el acceso.

Aunque idealmente dos resultados de dos cadenas de entrada distintas ingresados a una Función Hash no pueden ser iguales, en la realidad esto sí ocurre. Dos entradas de datos completamente distintas pueden generar el mismo hash, esto se le conoce con el nombre de **colisión** [12].

1.5.2.2 Cifrado de Llave Simétrica

La criptografía de llave simétrica es el método criptográfico que usa una misma clave, llave o contraseña para cifrar y descifrar mensajes. Las dos partes que se comunican han de ponerse de acuerdo de antemano sobre la clave a usar. Una vez que ambas tienen acceso a esta clave, el remitente cifra un mensaje usándola, lo envía al destinatario, y éste lo descifra con la misma clave [11].

El algoritmo para este proceso de cifrado sería el siguiente:

1. Ana y Beto acuerdan usar un algoritmo de cifrado.
2. Ana y Beto se ponen de acuerdo en que llave van a usar.
3. Ana cifra un mensaje con el algoritmo de cifrado y la llave acordada, creando así un mensaje cifrado.
4. Ana manda el mensaje cifrado a Beto.
5. Beto descifra el mensaje cifrado utilizando el algoritmo y la llave que habían acordado y obtiene el mensaje original.

El proceso de cifrado asimétrico sigue el proceso mostrado en la Figura 1.2:

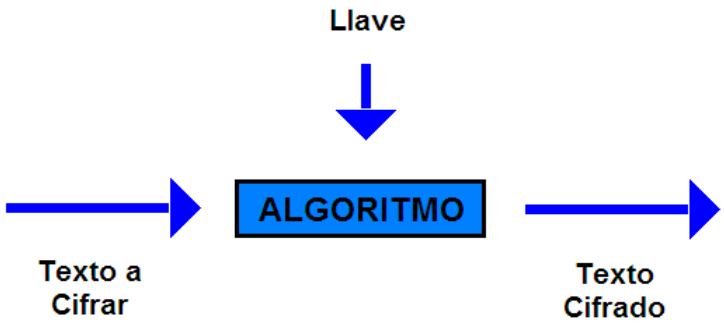


Figura 1.2 Proceso de Cifrado

Como se puede observar en la Figura 1.2, el proceso de cifrado toma como entrada un texto en claro, este pasa a través de un algoritmo de cifrado y con el uso de una llave de de cifrado es como se cifra la información.El proceso para descifrar el mensaje sigue el proceso mostrado en la Figura 1.3:

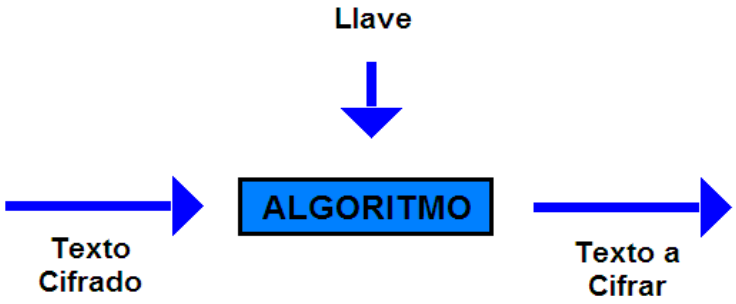


Figura 1.3 Proceso de Descifrado

Como se observa en la Figura 1.3, para descifrar un texto cifrado, se hace uso del mismo algoritmo y de la llave de cifrado con el que se cifró el texto, con lo cual se podrá obtener el texto original.

En este algoritmo es importante mantener la llave en secreto y que sólo sea conocida por quienes desean comunicarse. La llave debe de ser acordada en secreto ya que el conocimiento de la llave da acceso al conocimiento de todos los mensajes cifrados con ésta, y es ahí donde radica la debilidad de este tipo de cifrado, pues para ponerse de acuerdo sobre qué llave se va a utilizar, es necesario en ocasiones hacerlo a través de un medio público como lo es Internet, y debido a los problemas de seguridad que presenta Internet es posible que alguien más pueda obtener la llave de otras personas.

1.5.2.3 Cifrado de Llave Asimétrica

La criptografía asimétrica es el método criptográfico que usa un par de llaves para el envío de mensajes. Las dos llaves pertenecen a la misma persona a la que se ha

enviado el mensaje. Una llave es pública y se puede entregar a cualquier persona, la otra llave es privada y el propietario debe guardarla de modo que nadie tenga acceso a ella [11]. Las dos llaves que se usan en este tipo de cifrado tienen la particularidad de que si se cifra un mensaje con una llave, el mensaje cifrado solo puede ser descifrado con la otra llave.

El siguiente ejemplo muestra cómo se usa el cifrado de llave asimétrica:

1. Ana y Beto se ponen de acuerdo en un algoritmo de cifrado asimétrico.
2. Beto manda a Ana su llave pública.
3. Ana cifra un mensaje con la llave pública de Beto y se la envía a Beto.
4. Beto descifra el mensaje de Ana usando su llave privada.

Si Ana cifra primero el mensaje con su llave privada y Beto la descifra el mensaje con la llave pública de Ana, a ese proceso se conoce como **Firma Digital**, pues como solo Ana puede usar su llave privada para cifrar, solo ella pudo haber creado un mensaje que es posible descifrar con su llave pública.

A pesar de que el cifrado de llave asimétrica resuelve el problema del acuerdo de la llave en el cifrado simétrico, en la práctica no pueden sustituir al cifrado simétrico, ya que el cifrado asimétrico tiene desventajas tales como el hecho de que cifrar un mensaje es más lento, o que el mensaje cifrado es más largo. Es por esto que se pueden usar sistemas de cifrado híbridos, es decir, combinar el cifrado simétrico y el asimétrico. Esto se logra acordando mediante el cifrado asimétrico una llave entre dos entidades y utilizando posteriormente esta llave en el cifrado simétrico para cifrar la información.

1.5.3 Criptoanálisis

La palabra Criptoanálisis proviene de las palabras griegas “*kryptos*” que significa “palabra” y “*analyein*” que significa “para aflojar”, por lo cual, Criptoanálisis significa literalmente “aflojar la palabra”. Así como la criptografía se encarga de asegurar la información, el criptoanálisis es la ciencia de analizar y romper las comunicaciones seguras. El criptoanálisis envuelve una combinación de razonamiento analítico, aplicación de matemáticas, búsqueda de patrones, paciencia, determinación, y en ocasiones algo de suerte. A los criptoanalistas también se les llega a llamar atacantes [9].

La criptografía es empleada para implementar los servicios de seguridad, no obstante en el servicio de control de acceso los mecanismos no se basan en la criptografía, lo que se usa en este servicio son mecanismos de control de accesos, los cuales son:

- Listas de control de acceso: Son listas que contienen el nombre del usuario y los permisos que éste tiene.
- Información de autenticación: Puede ser el uso de passwords.

- Tiempo de acceso: Hace referencia a los períodos de tiempo en que un usuario puede tener acceso a determinados recursos o información.
- Duración del acceso: Se refiere al tiempo en que un usuario puede hacer uso de los recursos o información [8].

1.6 Conceptos de Seguridad sobre Análisis de Riesgos

Dada la complejidad del problema que representa la Seguridad Informática, para entenderla es necesario conocer algunos conceptos básicos:

- Activo

Es cualquier recurso de software, hardware, datos, de personal, de comunicaciones, etc. Por ejemplo: servidores, bases de datos, redes, usuarios, aplicaciones, sistemas operativos, información, etc. Dicho de otra forma, un activo es todo aquello que tiene valor para la empresa [1].

- Vulnerabilidad

Consiste en cualquier debilidad que puede explotarse para causar pérdida o daño al sistema. Indica que un activo es susceptible a recibir un daño a través de un ataque. Por ejemplo, falta de contraseñas en los equipos de la empresa, falta de registro de entradas y salidas en las instalaciones tanto de personal interno como externo, falta de políticas dentro de la empresa, falta de actualizaciones de los sistemas operativos y/o de las aplicaciones, etc. [1].

- Ataque

Consiste en cualquier acción que explota una vulnerabilidad. Existen dos tipos de ataques:

  - Ataques pasivos (sólo afectan la confidencialidad). Un ataque pasivo consiste sólo en monitorear la red, identificar como está constituida y obtener información importante a cerca de una empresa u organización sin alterar ni el estado del sistema ni la información. Aunque en esta etapa en sí, no se comete ninguna acción que afecte a la empresa, si se pasa a la vida real, es como si de repente se encontrase a una persona que está afuera de una empresa revisando qué puertas o qué ventanas están abiertas y por dónde se podría acceder a la empresa. Aunque en sí, no está ingresando a las instalaciones de la empresa, son actividades que hacen sospechar sobre las intenciones que se tienen al revisar los puntos de acceso a la empresa. Normalmente un ataque pasivo es realizado antes de realizar un ataque activo [13].

  - Ataques activos (afectan la confidencialidad, integridad y autenticidad). Un ataque activo tiene la capacidad de modificar o afectar la información, o el estado del sistema o ambos. Consiste en traspasar los mecanismos de

seguridad implementados en una empresa, acceder a información confidencial y la posterior destrucción, divulgación o modificación de la misma [13].

- Amenaza

Es cualquier circunstancia con el potencial suficiente para causar pérdida o daño al sistema. Existen diferentes tipos de amenazas: amenazas naturales (terremotos, inundaciones, huracanes, etc.), humanas, (huelgas, amenazas de bomba, empleados descontentos, etc.), y de tecnologías (hardware y software) [1].

- Riesgo

Es la probabilidad de que un evento desfavorable ocurra, tiene un impacto negativo si se materializa. Dependiendo del enfoque, el riesgo puede ser alto, medio, bajo o puede estar descrito en números, por ejemplo “el riesgo cuesta 150 mil pesos” [1].

- Control

Es cualquier acción que se tome para mitigar una amenaza. Por ejemplo desarrollo de políticas para el uso de los equipos, implementación firewalls e IDS´s, implementación de un plan de recuperación de desastres, creación de políticas de seguridad, capacitación y educación de los usuarios [1].

Para ejemplificar los conceptos anteriores se puede imaginar el siguiente escenario:

Existe una empresa que no cuenta con una adecuada política para el control del ingreso de personas externas, cierto día ingresa una persona externa que posee un teléfono celular que cuenta con una cámara digital lo suficientemente buena como para sacar imágenes nítidas de textos impresos, esta persona sin que nadie la vigile le saca fotos a documentos importantes para la empresa (como bien podría ser su cartera de clientes) y posteriormente vende esa información a otra empresa competidora, resultando todo esto en pérdidas económicas para la empresa.

En este ejemplo la vulnerabilidad viene siendo la falta de políticas para el control de personas externas a la empresa, la amenaza son las circunstancias que se derivan de las vulnerabilidades, que en este caso sería el hecho de que alguien entre a la empresa con una cámara digital. El riesgo es la probabilidad de que una amenaza se junte con una vulnerabilidad y se materialice, es decir, la probabilidad ya sea alta, media o baja de que alguien entre y obtenga fotos de información importante de la empresa. El impacto se da cuando a la empresa ingresa una persona con la cámara y obtiene información sensitiva de la empresa revelándola a un tercero, resultando en pérdidas económicas y/o de otra naturaleza, como bien pudiera ser la imagen de la empresa.

Otro ejemplo es el siguiente:

Es común escuchar “no camines de noche por tal zona porque corres el riesgo de que te asalten”.

La vulnerabilidad es el hecho de caminar en la noche por cierta zona. La amenaza es el hecho de poder ser asaltado. El riesgo es la probabilidad de sufrir un asalto; en este

caso la probabilidad aumenta por ser de noche. El impacto es cuando se es asaltado y se pierden pertenencias.

Estos últimos ejemplos por simples que parezcan, sirven para familiarizarse con la forma en que se identifican los activos, vulnerabilidades, amenazas y riesgos dentro del Análisis de Riesgos, el cual se verá más adelante.

En este capítulo se ha mencionado lo que es la Seguridad de la Información, se han descrito sus servicios y los mecanismos que permiten implementar los servicios de seguridad, y algunos conceptos que ayudarán más adelante a entender mejor el Análisis de Riesgos; sin embargo, la Seguridad Informática tiene un ciclo dividido en diferentes fases que se vuelven a repetir una vez que se ha llegado a la última fase, en el siguiente capítulo se explicará este proceso y sus diferentes etapas.

Referencias Capítulo 1

1 ISO/IEC 17799 **“Information Technology – Code of practice for information security management”.** Primera Edición. Estándar publicado por International Organization for Standardization en Suiza en el año 2000.

2 ITSecurity **“Top 10 Most Famous Hackers of All Time”.** Página Web disponible en: http://www.itsecurity.com/features/top-10-famous-hackers-042407/ Leído por última vez el 28 de septiembre de 2009.

3 Universidad de Alicante. **“VIRUS ILOVEYOU”.** Página Web disponible en: http://www.ua.es/es/novedades/comunicados/2000/iloveyou.htm Leído por última vez el 28 de septiembre de 2009.

4 VSantivirus “**Condenado el autor del virus Kournikova**”. Página Web disponible en: http://www.vsantivirus.com/29-09-01.htm Leído por última vez el 28 de septiembre de 2009.

5 *Eric A Fish, Gregory B. White* **“Secure Computers and Networks: Analysis, Design, and Implementation”.** Ed. CRC Press. Primera Edición. Publicado en Estados Unidos en el año 1999.

6 *Bill McCarty* **“El Libro oficial de Red Hat Linux firewalls”.** Ed. Anaya. Primera Edición. Publicado en España en el año 2003.

7 *James Michael Stewart* **“CISSP: Certified Information Systems Security Professional Study Guide”.** Ed. Tittel Mike Chapple. Tercera Edición. Publicado en Estados Unidos en el año 2005.

8 ISO 7498-2 **“Information processing systems - Open Systems Interconnection - Basic Reference Model Part 2 Security Architecture”.** Primera Edición. Estándar publicado por International Organization for Standardization en Suiza en el año 1989.

9 *Rolf Oppliger* **“Contemporary Cryptography”.** Ed. Artech House. Primera Edición. Publicado en Estados Unidos en el año 2005.

10 *Roberto Gómez Cárdenas* **“La esteganografía”.** Revista Bsecure. Editorial Netmedia. Publicada en México en el año 2004.

11 *Bruce Schneier* **“Applied Cryptography: Protocols, Algorithms, and Source Code in C”.** Ed John Wiley & Sons, Inc. Segunda Edición. Publicado en Estados Unidos en el año 1996.

12 *Magnus Daum, Stefan Lucks* **“Hash Collisions (The Poisoned Message Attack) "The Story of Alice and her Boss"”.** Página Web disponible en: http://th.informatik.uni-mannheim.de/People/lucks/HashCollisions/ Leído por última vez el 28 de septiembre.

13 *Enrique Daltabuit Godás, Leobardo Hernández Audelo, Guillermo Mallén Fullerton, José de Jesús Vázquez Gómez*. **“La seguridad de la información”.** Editorial Limusa Noriega Editores. Primera Edición. Publicado en México en el año 2007.

Capítulo

2

El Proceso Dinámico de la Seguridad Informática

Resumen

De la misma forma en que un proyecto de TI posee un ciclo de vida para poder ser implementado, también existe un ciclo de vida para los proyectos que tienen que ver con la Seguridad de la Información.

Implementar la seguridad en una empresa es un proceso que consta de diferentes etapas, este proceso es un ciclo que se repite constantemente, ya que cuando se ha terminado de implementar la seguridad en alguna organización habrán aparecido nuevos activos, nuevas amenazas y el ciclo comenzará de nuevo.

Aunque desde luego no es obligatorio conocer y seguir los pasos de un ciclo de vida para cualquier proyecto, sí resulta útil, pues ayuda a hacer las cosas de una forma estratégica y ordenada donde se optimizan tiempos y recursos.

En este capítulo se describe primero el ciclo de vida de la información y posteriormente se describirá el ciclo de vida de la Seguridad Informática, donde se mencionará en qué fase es que se encuentra localizado el Análisis de Riesgos.

---

2 El proceso Dinámico de la Seguridad Informática

Para comprender el ciclo de vida de la Seguridad Informática, es útil conocer también el Ciclo de Vida de la Información, el cual se explicará a continuación.

2.1 Ciclo de Vida de la Información

Existen diferentes tipos de información y por lo mismo hay información que siempre es valiosa, como la cartera de clientes de un banco; otro tipo de información es valiosa sólo en diferentes períodos, como por ejemplo, los registros del pago de la nómina de una empresa los cuales aumentan su valor los días anteriores a la quincena.

Sin embargo, toda la información tiene un ciclo de vida durante el cual la información es creada, procesada, transmitida y finalmente almacenada, aunque en algunos casos caerá en otras circunstancias tales como destrucción, maltrato, pérdida y corrupción [1].

La Figura 2.1 ilustra este ciclo.

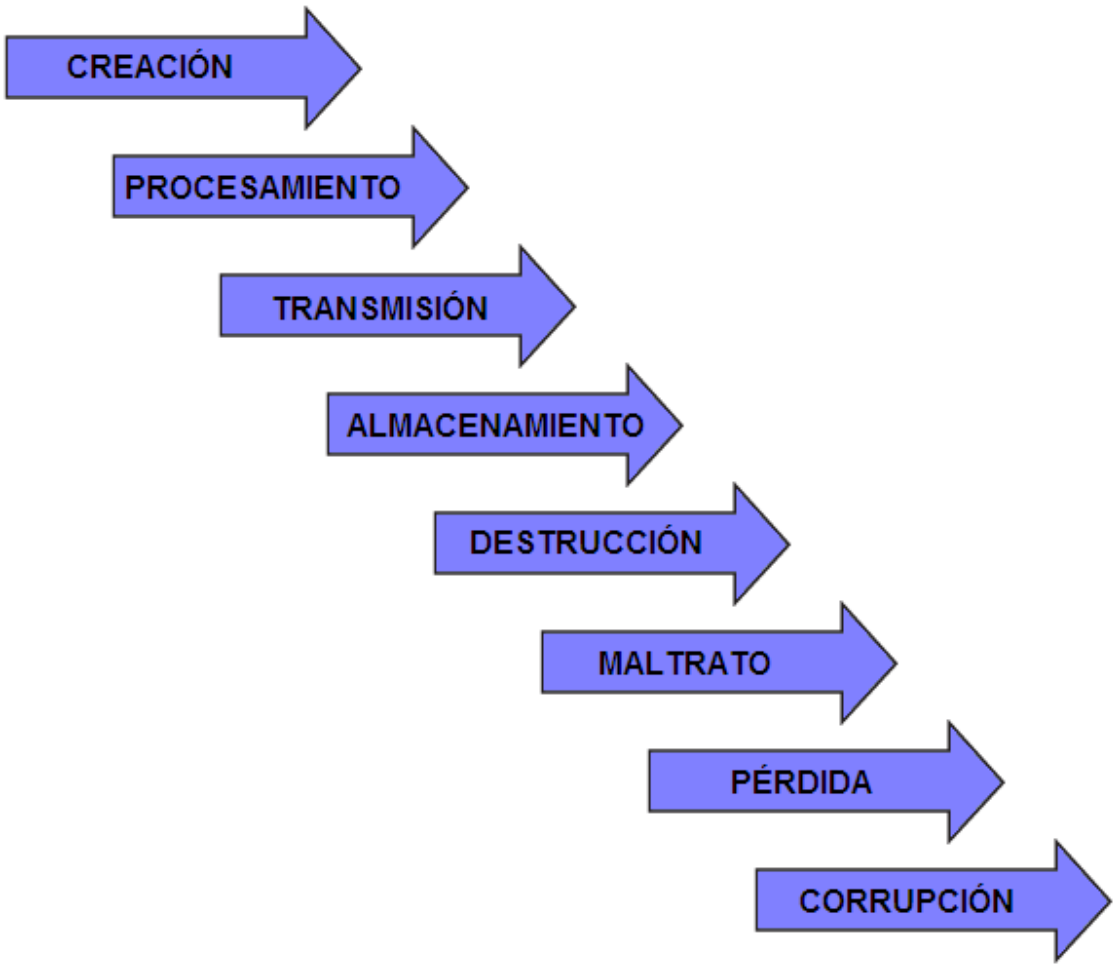


Figura 2.1 Ciclo de Vida de la Información

Las diferentes etapas del Ciclo de vida de la información mostradas en la Figura 2.1 se detallan a continuación:

2.1.1 Creación

La creación de la información está ligada con la adquisición de la información, la cual se adquiere por medio de los sentidos haciendo una recolección de datos, y después de su procesamiento es cuando se puede distinguir la información que resultará de dicho procesamiento, es de esta manera en que la información es creada.

2.1.2 Procesamiento

El procesamiento de la información consiste en tomar datos de entrada, procesarlos y en base a ello obtener información, la cual será necesaria para poder tomar decisiones.

2.1.3 Transmisión

La transmisión es realizada de distintas maneras, entre los seres humanos la información es transmitida mediante el lenguaje hablado o escrito, ya en medios electrónicos la información

es transmitida de distinta forma, pero se conserva el modelo de la comunicación, el cual consta de un emisor, un receptor, la información a transmitir, y de un medio de comunicación.

2.1.4 Almacenamiento

Desde la antigüedad ha sido necesario poder almacenar la información en algún medio, tales como pergaminos, libros e incluso canciones y relatos. Actualmente la información es almacenada en medios electrónicos siendo los discos duros los principales medios de almacenamiento. La finalidad de almacenar la información es poder conservarla para poder acceder a ella cuando sea necesario.

2.1.5 Destrucción

La destrucción de la información, ya sea de manera autorizada, accidental o maliciosa, consiste en borrar toda evidencia de que la información existió en alguna ocasión.

2.1.6 Maltrato

Este estado se refiere al mal uso de la información, por ejemplo cuando los empleados de un banco hacen uso de información confidencial propia de la empresa para su beneficio personal, que no necesariamente coincidirá con los intereses de la empresa.

2.1.7 Pérdida

La pérdida de la información se da cuando ya no es posible poder acceder a ella y no existe forma de recuperarla.

2.1.8 Corrupción

La corrupción de la información se da cuando ésta pierde su integridad, es decir, cuando la información pierde datos o se le insertan datos nuevos los cuales son llevados a cabo sin algún control que permita saber si los datos insertados son válidos o no.

Así como la información tiene un ciclo de vida donde la información se encuentra en diferentes estados, la seguridad de la información también tiene un ciclo de vida. El ciclo de vida de la Seguridad Informática es explicado desde diferentes puntos de vista, a continuación se explican dos de ellos.

2.2 Ciclo de Vida de la Seguridad Informática

Existen diferentes formas de describir el ciclo de vida de cualquier proceso, el NIST propone un ciclo que se describe a continuación:

2.2.1 Ciclo de Vida de la Seguridad propuesto por el NIST

El ciclo de vida propuesto por el *National Institute of Standards and Technology* (NIST) consta de 5 fases que se muestran en la Figura 2.2 [2]:

Figura 2.2 Ciclo de Vida de la Seguridad de la Información propuesta por el NIST

Las fases de las cuales consta el ciclo de vida mostrado en la Figura 2.2 son las siguientes:

2.2.1.1 Fase 1 Iniciación

En la primera fase se establece un compromiso con los socios del negocio, es decir, es necesario lograr concientizar a los altos directivos o dueños de la empresa, pues el apoyo de ellos es fundamental para poder analizar y comprender a la empresa a fin de conocer cuáles serán las áreas vulnerables.

En esta fase es útil realizar un Análisis de Riesgos informal, ya que si bien no arrojará todas las vulnerabilidades y amenazas a la empresa, los resultados serán suficientes para concientizar a cerca de que existen fallas que se deben de corregir. En esta fase también es útil documentar la arquitectura de la empresa, identificar las medidas de seguridad que se están aplicando tales como políticas o controles y categorizar la información que se maneja en los sistemas de información.

2.2.1.2 Fase 2 Adquisición / Desarrollo

En la segunda fase se realizará un Análisis de Riesgos, el cual mostrará las amenazas y vulnerabilidades que tiene la empresa así como las probabilidades de que éstas sean explotadas causando un daño a la empresa.

Con base en los resultados del Análisis de Riesgos se creará una guía de controles necesarios para la mitigación de los riesgos. Para poder seleccionar los controles que se implementarán es necesario realizar un reporte de costos para poder analizar la factibilidad de la implementación de los controles.

Para poder implementar los controles adecuados para la empresa es necesario realizar un plan donde se estimen los tiempos y los momentos adecuados para implementar los controles.

Por último en esta fase se realizan pruebas de seguridad y se evalúan los controles para saber que tan bien funcionarán una vez que sean acoplados a la operación de la empresa.

2.2.1.3 Fase 3 Implementación / Evaluación

En la tercera fase se aprobarán los productos y/o componentes que servirán como controles para la mitigación de los riesgos, así mismo se integrarán los controles a la operación de la empresa y se realizarán pruebas de seguridad para evaluar cómo se comporta el sistema con los controles implementados. Una vez que los riesgos hayan sido mitigados mediante la implementación de los controles adecuados, es necesario calcular el riesgo residual, el cual viene siendo el porcentaje del riesgo que el control no pudo terminar de mitigar.

Un aspecto importante en esta fase es orientar y capacitar a los usuarios y administradores para que conozcan las nuevas medidas de seguridad.

Dependiendo del tipo de institución, puede estar o no obligada a cumplir con determinadas certificaciones, para lo cual es necesario acreditar que se está cumpliendo con un mínimo de requisitos que solicite la certificación correspondiente.

2.2.1.4 Fase 4 Operación / Mantenimiento

La cuarta fase consiste en la operación y mantenimiento. En esta fase es necesario realizar un monitoreo continuo para revisar que los controles estén funcionando correctamente y para detectar posibles intrusos que pudiesen intentar realizar acciones no autorizadas. En esta fase también es necesario llevar un control sobre los incidentes que ocurren en la operación diaria así como un control de cambios realizados, dichas acciones facilitarán la ejecución de una auditoría. Una auditoria no debe ser vista como algo negativo, pues su finalidad es identificar las áreas que pueden ser mejoradas así como identificar donde están funcionando mejor los controles elegidos para la mitigación de los riesgos.

2.2.1.5 Fase 5 Ocaso

En esta última fase se planea la transición para volver a iniciar de nuevo el ciclo. Se realizará la documentación de todo lo que se ha hecho durante este ciclo y se resguardará para poderla consultar más adelante cuando sea necesario.

Es importante también que si se van a eliminar diferentes medios donde se haya almacenado información sensitiva, estos sean sanitizados, es decir, que de ellos no se pueda extraer información sensitiva que hayan contenido anteriormente. Dicha acción no resulta tan trivial ya que los dispositivos de almacenamiento, tales como discos duros, pueden seguir almacenando información incluso después de que hayan sido formateados; es necesario el uso de herramientas para asegurar que los medios hayan sido sanitizados e incluso si es necesario se deberán de destruir los medios.

Este Ciclo de vida propuesto por el NIST no es el único, hay otro ciclo de vida igualmente interesante propuesto por el Instituto SANS.

2.2.2 Ciclo de Vida de la Seguridad propuesto por el SANS

Este modelo ha sido desarrollado por el Instituto *SysAdmin Audit Network Security* (SANS) el cual consta de 4 fases, que es el que se muestra en la Figura 2.3.

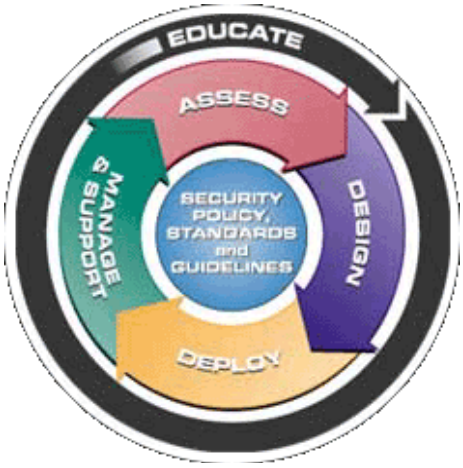


Figura 2.3 Ciclo de Vida de la Seguridad propuesta por el SANS

Las fases del Ciclo de Vida de la Seguridad mostradas en la Figura 2.3 son las siguientes:

La primera fase es la evaluación, considerada como un acontecimiento crucial que determina el proyecto de ley en seguridad, que determina, a su vez, la salud de cualquier sistema.

Actividades como son auditorias, pruebas de penetración y revisiones, se llevarán a cabo periódicamente o cuando surjan necesidades, tal es el caso de un cambio importante.

Normalmente la evaluación de riegos se calcula a partir de los datos recabados.

El diseño es la segunda fase del ciclo de vida, se basa en la organización y las normas de la industria, esta etapa provee una adecuada configuración de seguridad, el diseño comprende actividades como la formulación y el proceso de mejora con respecto al diseño en sí.

La implementación es la tercera fase, la cual consiste en desplegar el diseño elaborado en la etapa o fase anterior. Especialistas y personal calificado deben de ser empleados para estas actividades.

Por último, la administración y el monitoreo son fundamentales para asegurar que el sistema sea funcional y ayuda de manera proactiva como un mecanismo de detección de problemas.

Es importante contar con capacitación continua en todo el ciclo de vida en los diferentes niveles organizacionales, las aptitudes y conocimiento se plantearán dentro de este proceso [3].

En este capítulo se mencionó el ciclo de vida de la Seguridad Informática, que como se vio cuenta con diferentes actividades, las cuales no carecen de cierta complejidad. Para muchas de estas actividades es recomendable apegarse a estándares, que si bien por sí mismos no garantizarán la ausencia de errores, por lo menos servirán para realizar diferentes actividades basándonos en un método que ya ha sido probado. En el siguiente capítulo se describirán diferentes estándares relacionados con la Seguridad de la Información y se explicarán diferentes tipos de controles que existen para poder implementar la seguridad.

Referencias Capítulo 2

1 *Leonardo García Rojas* **“The information security process under BS7799/ISO17799”.** Paper Publicado en la Conferencia de Nebraska Cert 2005 realizada en Estados Unidos en el año 2005. Disponible en http://www.certconf.org/presentations/2005/files/WA1.pdf

2 *Computer Security Division NIST* **“INFORMATION SECURITY IN THE SYSTEMS DEVELOPMENT LIFE CYCLE”** Versión 2. Publicado por el National Institute of Standards and Technology en Estados Unidos en el año 2007. Disponible en http://csrc.nist.gov/groups/SMA/sdlc/index.html

3 *Lee Wan Wai* **“Security Life Cycle”.** White Paper. Versión 1. Publicado por SANS Institute en Estados Unidos en el año 2001. Disponible en http://www.sans.org/reading_room/whitepapers/testing/security_life_cycle_1_diy_assessment_260?show=260.php&cat=testing

Capítulo

3

Estándares y Controles de Seguridad

Resumen

Dada la complejidad de las empresas y la dificultad para proteger sus activos, es recomendable apegarse a una norma o estándar que sirva de guía para disminuir los riesgos.

Actualmente hay diferentes instituciones que se encargan de desarrollar estándares y normas de seguridad, una de ellas es *International Organization for Standardization* (ISO). ISO es conocida por crear normas internacionales de fabricación, comercio y comunicación para diferentes ramas de la industria. ISO tiene diferentes estándares de seguridad que pueden ser muy útiles en el área de la Seguridad Informática, no obstante para poder tener acceso a ellos es necesario pagar cierta cantidad de dinero por cada documento al que se quiera accesar.

Otra organización que también se encarga de desarrollar estándares de seguridad es el *National Institute of Standards and Technology* (NIST) en los Estados Unidos. El NIST ha creado diferentes lineamientos que principalmente van dirigidos a instituciones del gobierno de los Estados Unidos, no obstante muchas de ellas pueden aplicarse en diferentes instituciones. Es posible acceder a las publicaciones del NIST a través de su página de forma gratuita.

Otro tema que abarca este capítulo son los controles. La selección e implementación de los controles de seguridad es una de las tareas más importantes en la implementación de la seguridad de la información ya que de una adecuada selección de controles dependerá la correcta mitigación de riesgos.

---

3 Estándares y Controles de Seguridad

3.1 Estándares de Seguridad

A continuación se dará una descripción de los estándares de seguridad más conocidos dentro del ámbito de la seguridad de la información.

3.1.1 ISO 17799:2000

El ISO 17799 es un estándar creado por dos organismos internacionales: International Electrotechnnical Commission (IEC) e ISO, que ya se menciono anteriormente. Ambos organismos participan en el desarrollo de estándares internacionales y en el campo de la tecnología de la información. ISO e IEC han establecido un comité técnico conjunto, ISO/IEC [1].

Al ser un estándar, es posible aplicarlo en la mayoría de las organizaciones y en diferentes escenarios, ya sea en empresas de gobierno, en la iniciativa privada o en instituciones educativas. Dependiendo de los objetivos de cada empresa se dará un énfasis especial a algún área de este estándar.

Este estándar define la Seguridad Informática y menciona algunas razones por las cuales es necesario proteger la información, e igual de importante, menciona que puntos de inicio se pueden considerar para implementar la seguridad de la información. La definición de Seguridad Informática que ofrece este estándar es la que se dio en el capítulo 1.

De acuerdo con este estándar, los requerimientos de seguridad se pueden obtener evaluando los riesgos para la organización sin dejar de lado la estrategia general y los objetivos de la organización. Al evaluar el riesgo se identifican las amenazas para los activos, se evalúa la vulnerabilidad y el riesgo, y en base a eso se calcula el impacto que podría tener.

El riesgo se debe identificar, cuantificar y priorizar, y en base al resultado de esto se determinará la gestión apropiada y las prioridades para manejar los riesgos de la información. Este estándar menciona que la evaluación de riesgos se puede aplicar a toda la organización, sólo a unas partes de la organización, o a un sistema de información individual; no obstante, se obtienen mejores resultados si la evaluación de riesgos abarca a toda la empresa. Una vez evaluado el riesgo se deberá determinar si se pueden aceptar los riesgos o si es necesario tomar otras acciones. Un riesgo se puede aceptar si el riesgo es bajo o el costo de mitigarlo es muy alto.

Para cada uno de los riesgos que se hayan identificado dentro de la organización se deberá de tomar la decisión de cuál será su tratamiento, los posibles tratamientos que menciona este estándar son los siguientes:

- Controlar el riesgo
- Aceptar el riesgo
- Evitar el riesgo
- Transferir el riesgo

Si la decisión es controlar el riesgo los controles deberán asegurar que los riesgos se reduzcan a un nivel aceptable.

Este estándar además describe 10 áreas de seguridad que son las siguientes:

1. Políticas de seguridad. El estándar define que las políticas de seguridad deben de ser obligatorias, así como la documentación de procedimientos internos de la organización que permitan su actualización y revisión por parte de un Comité de Seguridad.

2. Seguridad organizacional. Establece el marco formal de seguridad que debe integrar una empresa, tales como un foro de administración de la seguridad de la información, un oficial de seguridad, revisiones externas a la infraestructura de seguridad y controles a los servicios de personas externas a la empresa, entre otros aspectos.

3. Clasificación y control de activos. Se realizará un Análisis de Riesgos el cual generará un inventario de activos que deberá ser administrado y controlado con base en ciertos criterios de clasificación y etiquetado de información, es decir, los activos serán etiquetados de acuerdo con su nivel de confidencialidad.

4. Seguridad del personal. Esta área se enfoca a proporcionar controles para las acciones del personal que opera con los activos de información. El objetivo de esta área del estándar es contar con los elementos necesarios para mitigar el riesgo inherente a las actividades humanas, es decir, se deberán establecer claras responsabilidades por parte del personal en materia de seguridad de la información.

5. Seguridad física y de entorno. Es necesario identificar los perímetros de seguridad, de forma que se puedan establecer controles en el manejo de equipos, transferencia de información y control de los accesos a las distintas áreas con base en el tipo de seguridad establecida.

6. Comunicaciones y administración de operaciones. Esta área trata acerca de integrar los procedimientos de operación de la infraestructura tecnológica y de controles de seguridad, que van desde el control de cambios en la configuración de los equipos, manejo de incidentes, administración de aceptación de sistemas, hasta el control de código malicioso.

7. Control de acceso. Se deberán habilitar mecanismos que permitan monitorear el acceso a los activos de información, los cuales incluyen los procedimientos de administración de usuarios, definición de responsabilidades o perfiles de seguridad y el control de acceso a las aplicaciones.

8. Desarrollo de sistemas y mantenimiento. La empresa deberá disponer de procedimientos que garanticen los sistemas en cuanto a calidad y para tareas específicas de la organización.

9. Continuidad de las operaciones de la organización. El sistema de administración de la seguridad debe integrar en sus procedimientos planes de recuperación de desastres y planes para la continuidad del negocio, los cuales deberán ser revisados de manera constante y puestos a prueba con la finalidad de determinar las limitaciones de los mismos y verificar su correcto funcionamiento.

10. Cumplimiento de requerimientos legales. La organización establecerá los requerimientos de seguridad que deben cumplir todos sus proveedores, socios y usuarios; éstos se encontrarán formalizados en los contratos o convenios.

Cada una de estas áreas contienen diferentes categorías de controles de seguridad que incluyen el objetivo que el control debe de alcanzar y uno o más controles que se pueden aplicar para lograr el objetivo del área.

Este estándar fue actualizado en el año 2005, en la versión 2005 se agrega un área más, la cual se llama “Administración de Incidentes de Seguridad Informática” cuya finalidad es asegurar que cualquier incidente de seguridad sea reportado a tiempo para poder tomar acciones correctivas.

3.1.2 ISO 27001

Este estándar tiene su origen en la segunda parte del BS 7799, el cual fue desarrollado por la entidad de normalización británica *British Standards Institution* (BSI) [2].

El ISO 27001 es un estándar aceptado internacionalmente para la administración de la seguridad de la información. Su título completo es BS 7799-2:2005 (ISO/IEC 27001:2005).

Esta norma no está orientada a aspectos técnicos sino a aspectos organizativos, es decir, tiene por objetivo organizar la seguridad de la información, debido a ello propone acciones de establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del *Information Security Management System* (ISMS) conocido en México como Sistema Administrativo de Seguridad Informática.

Este estándar cubre diferentes tipos de organizaciones, por ejemplo: empresas comerciales, empresas de gobierno, o empresas no lucrativas, sin importar si son empresas pequeñas o grandes.

Es necesario entender los requerimientos de seguridad de la información de una organización para así poder establecer los objetivos para la seguridad de la información e implementar y operar controles para administrar los riesgos de Seguridad Informática de una organización en el contexto de los riesgos de negocio sobre toda la organización, también es necesario monitorear y revisar el rendimiento y efectividad del ISMS y hacer una mejora continua basándose siempre en los objetivos de la empresa.

Este estándar internacional adopta el modelo "*Plan-Do-Check-Act*" (PDCA), el cual es aplicado a toda la estructura de procesos de ISMS de la siguiente forma:

- Plan (Establecer el ISMS): Implica establecer las políticas del ISMS, sus objetivos, procesos, procedimientos relevantes para la Administración de Riesgos y mejoras para la seguridad de la información, entregando resultados acordes a las políticas y objetivos de toda la organización.

- Do (Implementar y operar el ISMS): Representa la forma en que se deben operar e implementar las políticas, controles, procesos y procedimientos.

- Check (Monitorizar y revisar el ISMS): Consiste en analizar y medir, donde sea aplicable, los procesos ejecutados con relación a la política del ISMS, evaluar objetivos, experiencias e informar los resultados a la administración para su revisión.

- Act (Mantener y mejorar el ISMS): Se refiere a realizar las acciones preventivas y correctivas, basadas en las auditorías internas y revisiones del ISMS o cualquier otra información relevante para permitir la mejora continua del ISMS.

La Figura 3.1 muestra el modelo PDCA aplicado al proceso ISMS:

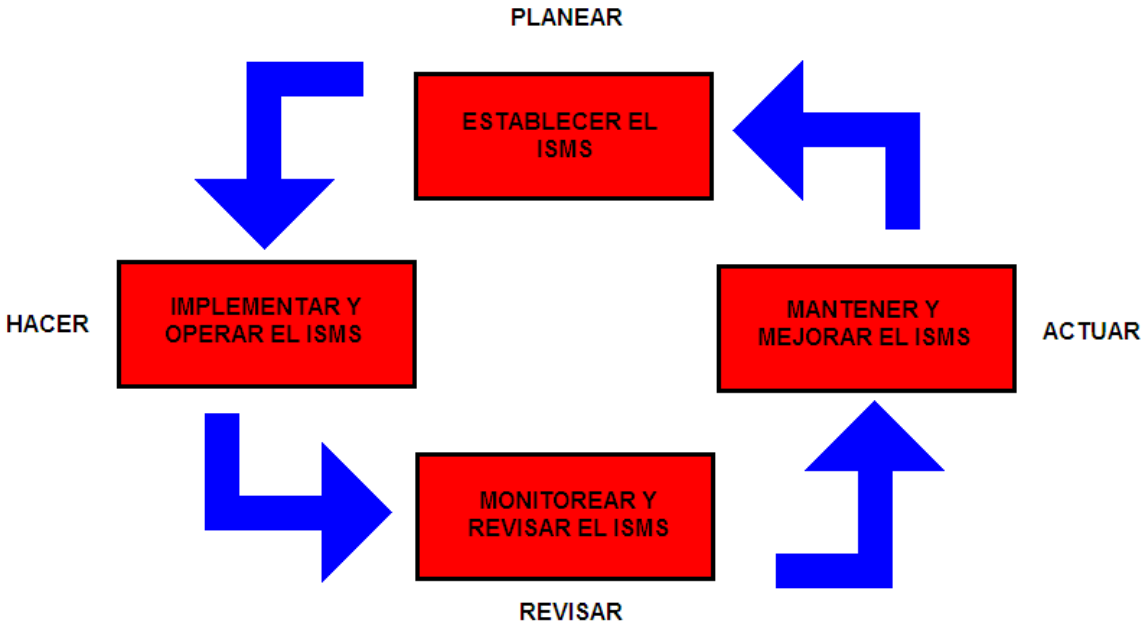


Figura 3.1 Modelo PDCA aplicado al ISMS

A continuación se describe el modelo PDCA mostrado en la Figura 3.1.

En la fase de **Planeación** que consiste en el **Establecimiento del ISMS**, el estándar da los pasos a seguir que son los siguientes:

1. Establecer el objetivo y los límites en función de las características del negocio, la organización, los activos, la ubicación, tecnología, e incluir una justificación del objetivo.

2. Definir una política para el ISMS de acuerdo a las características del negocio que incluya una estructura para los objetivos que se desean alcanzar.

3. Definir un Análisis de Riesgos enfocado a la organización. Para esto se debe escoger una metodología que se adapte al ISMS y a los requerimientos del negocio. Se debe también de desarrollar un criterio para saber si un riesgo se puede aceptar e identificar qué niveles de riesgo se pueden aceptar.

4. Identificar los riesgos. En este paso se identifican los activos, las amenazas para los activos, las vulnerabilidades que podrían ser explotadas por las amenazas, y los impactos ocasionados en caso de que se perdiera la confidencialidad, integridad y disponibilidad de la información.

5. Analizar y evaluar los riesgos. Se debe evaluar el impacto que tendrá para la organización el hecho de que falle la seguridad, tomando en cuenta las consecuencias de la pérdida de la confidencialidad, integridad y disponibilidad de los activos.

6. Identificar y evaluar opciones para mitigar los riesgos. Estas opciones son aplicar

controles, aceptar el riesgo, evitar el riesgo o transferir el riesgo.

7. Seleccionar los controles para mitigar los riesgos. En esta selección se deberán de tomar en cuenta el criterio de aceptación de riesgos y requerimientos legales y regulatorios.

8. Obtener la aprobación de la gerencia.

9. Preparar un documento donde se identifiquen los controles seleccionados y donde se explique cómo y por qué son apropiados.

En la fase de **Implementación y Operación** del ISMS, la organización deberá de hacer lo siguiente:

- Formular un plan para la mitigación de riesgos que identifique una apropiada administración de acciones, recursos, responsabilidades y prioridades para administrar los riesgos de Seguridad Informática.

- Implementar el plan de mitigación de riesgos.

- Implementar los controles seleccionados en la fase de planeación para conocer los objetivos de control.

- Determinar que tan efectivos son los controles al momento de proteger a los activos.

- Implementar planes de capacitación y entrenamiento.

- Administrar las operaciones del ISMS.

- Administrar los recursos para el ISMS.

- Implementar procedimientos y otros controles capaces de permitir la detección de incidentes de seguridad y responder a dichos incidentes.

En la fase de **Revisión** es donde se **Monitorea y se Revisa el ISMS**. En esta fase la organización deberá hacer lo siguiente:

- Realizar el monitoreo y la revisión de procedimientos y otros controles para:

    - Detectar errores en los resultados de procesamiento.
    - Identificar incidentes de seguridad, ya sea que hayan tenido éxito o no.
    - Permitir a la administración determinar si las actividades de seguridad delegadas a personas o implementadas mediante TI están funcionando como se esperaba.
    - Ayudar a detectar eventos de seguridad y prevenir incidentes de seguridad a través del uso de identificadores.
    - Determinar cuáles de las acciones tomadas para resolver los problemas de

seguridad fueron efectivos.

- Revisar regularmente la efectividad del ISMS tomando en cuenta los resultados de auditorías en seguridad, incidentes, de las medidas de efectividad, sugerencias y recomendaciones de todas las partes interesadas.

- Medir la efectividad de los controles para verificar que los requerimientos de seguridad están siendo cubiertos.

- Revisar la Administración de Riesgos en intervalos preestablecidos y revisar el nivel del riesgo residual tomando en cuenta cambios en:

    - La organización.
    - Tecnología.
    - Objetivos del negocio y procesos.
    - Amenazas identificadas.
    - Efectividad de los controles implementados.
    - Eventos externos tales como cambios en marcos regulatorios o legales, cambios en el ámbito social.

- Realizar auditorías internas al ISMS en intervalos preestablecidos.

- Realizar una revisión de la administración del ISMS de manera regular para garantizar que las acciones tomadas siguen siendo adecuadas.

- Actualizar los planes de seguridad.

- Registrar acciones y eventos que pudieran haber impactado en la efectividad o el rendimiento del ISMS.

La última fase consiste en el Mantenimiento y Mejora del ISMS. La organización deberá hacer regularmente lo siguiente:

- Implementar las mejoras identificadas en el ISMS.

- Tomar acciones correctivas y preventivas para:

    - Eliminar la causa de disconformidades con los requerimientos del ISMS.
    - Prevenir acciones que conducirían al impacto de problemas potenciales.

- Hacer saber a las partes interesadas de las mejoras y pruebas realizadas.

- Asegurarse de que las mejoras cumplen con los objetivos deseados.

3.1.3 ISO 7498-2

Este estándar es la continuación del ISO 7498, el cual describe el modelo OSI. El objetivo del modelo OSI es permitir la interconexión de diferentes computadoras en un medio abierto [3].

El ISO 7498-2 define los elementos relacionados con una arquitectura de seguridad que puede ser aplicada en circunstancias en las que se requiera protección para un sistema abierto. Éste estándar proporciona una descripción general de los servicios de seguridad y sus respectivos mecanismos que pueden ser implementados, también describe donde se pueden usar dichos servicios y mecanismos.

Este estándar identifica cinco clases de servicios de seguridad: Confidencialidad, Autenticación, Integridad, Control de Acceso, y No Repudio, los cuales a su vez tienen diferentes clasificaciones, que son las siguientes:

3.1.3.1 Confidencialidad

El estándar 7498-2 clasifica el servicio de confidencialidad en 4 tipos:

- **Confidencialidad orientada a conexión**: Consiste en la protección de todos los datos de usuario en una comunicación orientada a una conexión.

- **Confidencialidad no orientada a conexión**: Viene siendo la protección de todos los datos de usuario contenidos en una sola unidad de datos del servicio en una comunicación no orientada a conexión.

- **Confidencialidad selectiva**: Se refiere a la protección de campos específicos de todas las unidades de datos de usuario de una comunicación orientada a conexión o de una sola unidad de datos del servicio en una comunicación no orientada a conexión.

- **Confidencialidad aplicada al análisis del tráfico**: Este servicio sirve para la protección de los datos frente a un análisis del tráfico originado por una comunicación entre entidades pares. Así, un intruso podría analizar las direcciones, origen y destino de las unidades de datos intercambiadas, la cantidad de datos transmitidos y la frecuencia con que tiene lugar la comunicación entre entidades pares.

3.1.3.2 Autenticación

El servicio de Autenticación es clasificado en dos tipos:

- **Autenticación de entidades pares**: Este servicio se aplica a comunicaciones orientadas a conexión. Al establecerse la conexión, este servicio asegura la identidad de las dos entidades que se comunican, es decir, se asegura que cada una es quién dice ser. Posteriormente, en la fase de transferencia debe garantizar que un intruso no pueda suplantar a cualquiera de las dos entidades legítimas.

- **Autenticación de origen de datos**: Este servicio se aplica a comunicaciones no orientadas a conexión donde las unidades de datos son independientes y por lo tanto en este caso lo más que se puede garantizar es que el origen de cada unidad de datos corresponde con la indicada en su cabecera. Este servicio puede ofrecerse en aplicaciones como el correo electrónico, donde no hay una comunicación previa entre entidades finales.

3.1.3.3 Integridad

El servicio de Integridad es clasificado en 5 tipos:

- **Integridad orientada a conexión con mecanismos de recuperación**: Proporciona la integridad de todos las unidades de datos de usuario de una comunicación orientada a conexión y detecta cualquier modificación, inserción, borrado o retransmisión de cualquier unidad de datos dentro de una secuencia entera de unidad de datos del servicio haciendo uso de mecanismos de recuperación de la integridad si fuera necesario.

- **Integridad orientada a conexión sin mecanismos de recuperación**: Este servicio es semejante al anterior con la diferencia de que en este caso sólo se detectan las violaciones en la integridad de los datos, pero no se articulan mecanismos de recuperación de la integridad.

- **Integridad orientada a conexión sobre campos selectivos**: Este servicio asegura la integridad de campos específicos dentro de las unidades de datos de usuario en una comunicación orientada a una conexión, y toma una determinación de si los campos seleccionados han sido modificados, insertados, borrados o retransmitidos.

- **Integridad no orientada a conexión**: Este servicio asegura la integridad de una sola unidad de datos del servicio en comunicaciones no orientadas a conexión, teniendo alguna forma de detección de la modificación de una unidad de datos del servicio.

- **Integridad no orientada a conexión sobre campos selectivos**: Este servicio asegura la integridad de campos específicos dentro de una sola unidad de datos del servicio en comunicaciones no orientadas a conexión. Este servicio toma alguna determinación si los campos seleccionados han sido modificados.

3.1.3.4 Control de Acceso

El control de acceso protege a los activos del sistema contra accesos y uso no autorizados. De todos los servicios contemplados en este estándar, el servicio de Control de Acceso es el único que no requiere el uso de la criptografía para su implementación. Para su implementación existe un gran número de técnicas propias y tipos de control de acceso, así como también modelos específicos para su implementación.

3.1.3.5 No Repudio

El servicio de No Repudio está clasificado en dos tipos:

- No repudio del origen. Este servicio proporciona los mecanismos necesarios para asegurar que el mensaje fue enviado por la entidad especificada.

- No repudio del destino. Este servicio proporciona los mecanismos necesarios para asegurar que el mensaje fue recibido por la entidad especificada.

En la Tabla 3.1 se muestran los mecanismos que pueden ser usados para poder implementar los servicios de seguridad:

	Mecanismo							
Servicio	Cifrado	Firma Digital	Control de Acceso	Integridad de los datos	Intercambio de autenticación	Relleno de tráfico	Control de Ruteo	Notarización
Autenticación de entidades pares	S	S	N	N	S	N	N	N
Autenticación de origen de datos	S	S	N	N	N	N	N	N
Control de acceso	N	N	S	N	N	N	N	N
Confidencialidad orientada a conexión	S	N	N	N	N	N	S	N
Confidencialidad no orientada a conexión	S	N	N	N	N	N	S	N
Confidencialidad selectiva	S	N	N	N	N	N	N	N
Confidencialidad en el flujo de tráfico	S	N	N	N	N	S	S	N
Integridad con conexión con recuperación	S	N	N	S	N	N	N	N
Integridad con conexión sin recuperación	S	N	N	S	N	N	N	N
Integridad con conexión selectiva a campos	S	N	N	S	N	N	N	N
Integridad sin conexión	S	S	N	S	N	N	N	N
Integridad sin conexión selectiva a campos	S	S	N	S	N	N	N	N
No repudio del origen	N	S	N	S	N	N	N	S
No repudio del destino	N	S	N	S	N	N	N	S

S Si: El Mecanismo es considerado apropiado para el servicio
N No: El Mecanismo no es considerado apropiado para el servicio

Tabla 3.1 Mecanismos y Servicios de Seguridad

Algunos de los mecanismos de seguridad descritos en la Tabla 3.1 ya han sido vistos en el capítulo 1, tales como el cifrado o la firma digital. Los mecanismos que no se han visto se describen a continuación:

3.1.3.6 Control de Acceso

Los **mecanismos de control de acceso** pueden basarse, por ejemplo, en la utilización de uno o más de los elementos siguientes:

a. Bases de información de control de acceso, donde se mantienen los derechos de acceso de entidades pares. Esta información debe ser mantenida por centros de autorización o por la entidad a la que se accede, y puede tener la forma de una lista de control de acceso o de una matriz de estructura jerárquica o distribuida. Esto presupone que se ha asegurado la autenticación de la entidad par.
b. Información de autenticación como contraseñas, cuya posesión y presentación son la prueba de la autorización de la entidad que efectúa el acceso.
c. Capacidades, cuya posesión y presentación son la prueba del derecho a acceder a la entidad o recurso definido por la capacidad.
d. Etiquetas de seguridad, que cuando están asociadas con una entidad, pueden utilizarse para conceder o negar el acceso, en general de acuerdo con una política de seguridad.
e. Hora del intento de acceso.
f. Ruta del intento de acceso.
g. Duración del acceso.

Pueden aplicarse mecanismos de control de acceso en cualquiera de los dos extremos de una asociación de comunicaciones y/o cualquier punto intermedio.

Los controles de acceso aplicados en el origen con cualquier punto intermedio se utilizan para determinar si el emisor está autorizado a comunicar con el destinatario (receptor) y/o a utilizar los recursos de comunicaciones requeridos.

En una transmisión de datos en modo sin conexión, los requisitos de los mecanismos de control de acceso de la entidad par en el destino, deben conocerse con prioridad en el origen, y deben registrarse en la base de informaciones de gestión de seguridad.

3.1.3.7 Integridad de los Datos

La integridad de los datos tiene dos aspectos: la integridad de una sola unidad de datos o de un solo campo, y la integridad de un tren de unidades de datos o de campos de unidad de datos. En general, se utilizan diferentes mecanismos para proporcionar estos dos tipos de servicios de integridad, aunque no es práctica la provisión del segundo sin el primero.

La determinación de la integridad de una sola unidad de datos entraña dos procesos, uno en la entidad emisora y otro en la entidad receptora. La entidad emisora añade a una unidad de datos una cantidad que es una función de los propios datos. Esta cantidad puede ser una información suplementaria, tal como un código de control de bloque o un valor de control criptográfico, y puede estar cifrada. La entidad receptora genera una cantidad correspondiente y la compara con la cantidad recibida para determinar si los datos han sido

modificados en tránsito; este mecanismo por sí solo no ofrecerá protección contra la reproducción de una sola unidad de datos. En las capas apropiadas de la arquitectura, la detección de una manipulación puede conducir a una acción de recuperación (por ejemplo, una retransmisión o una corrección de error) en esa capa o en otra superior.

Para la transferencia de datos en modo con conexión, la protección de la integridad de una secuencia de unidades de datos (es decir, la protección contra errores de secuenciación, pérdida, reproducción, inserción o modificación de datos) requiere además alguna forma de ordenación explícita, como la numeración de secuencias, el estampado de la hora (*time stamping*) o el encadenamiento criptográfico.

Para la transmisión de datos en modo sin conexión, el estampado de la hora puede utilizarse para proporcionar una forma limitada de protección contra la reproducción de unidades de datos individuales.

3.1.3.8 Intercambio de Autenticación

Algunas de las técnicas que pueden aplicarse a los intercambios de autenticación son:

a. Utilización de información de autenticación, como contraseñas, suministradas por una entidad emisora y verificadas por la entidad receptora.
b. Técnicas criptográficas.
c. Uso de características y/o propiedades de la entidad.

Los mecanismos pueden incorporarse en la capa (N) para proporcionar autenticación de la entidad par. Si el mecanismo no logra autenticar la entidad, el resultado será el rechazo o la terminación de la conexión y puede causar también una anotación en el registro de auditoría de seguridad y/o un informe a un centro de gestión de seguridad.

Cuando se utilizan técnicas criptográficas, éstas pueden combinarse con protocolos de toma de contacto: como protección contra la repetición (es decir, asegurar el funcionamiento en tiempo real). Mediante el estampado de la hora y relojes sincronizados (GPS);

a. Dos o tres tomas de contacto (para autenticación unilateral y mutua respectivamente).

b. Servicios de no repudio, mediante firma digital y mecanismos de notarización.

3.1.3.9 Relleno de Tráfico

Pueden utilizarse mecanismos de relleno de tráfico para proporcionar diversos niveles de protección contra análisis del tráfico. Este mecanismo puede ser eficaz solamente si el relleno de tráfico está protegido por un servicio de confidencialidad.

3.1.3.10 Control de Ruteo

Las rutas pueden elegirse dinámicamente o por acuerdo previo con el fin de utilizar sólo

subredes, relevadores o enlaces físicamente seguros. Al detectar ataques de manipulación persistentes, los sistemas extremos pueden dar instrucciones al proveedor del servicio de red que establezca una conexión por una ruta diferente.

La política de seguridad puede prohibir que los datos que transportan ciertas etiquetas de seguridad pasen a través de ciertas subredes, relevadores o enlaces. Asimismo, el iniciador de una conexión (o el expedidor de una unidad de datos en modo sin conexión) puede especificar prohibiciones de encaminamiento en las que se indica que se eviten determinadas subredes, enlaces o relevadores.

3.1.3.11 Notarización

Pueden garantizarse las propiedades sobre los datos comunicados entre dos o más entidades, tales como su integridad, origen, fecha y destino, mediante la provisión de un mecanismo de notarización. La seguridad es proporcionada por una tercera parte que actúa como notario, en el que las entidades comunicantes tienen confianza y que mantiene la información necesaria para proporcionar la garantía requerida de una manera verificable; cada instancia de comunicación puede utilizar la firma digital, el cifrado y los mecanismos de integridad, según sea apropiado, para el servicio que es proporcionado por el notario. Cuando se invoca este mecanismo de notarización, los datos se comunican entre las entidades comunicantes por las instancias de comunicación protegidas y el notario.

3.1.4 Orange Book

Orange Book es uno de los libros más significantes de *Rainbow Series* publicados por el gobierno de los Estados Unidos, los cuales fueron publicados originalmente por el Departamento de Defensa de los Estados Unidos. Este libro también es conocido como "*Trusted Computer System Evaluation Criteria*" (TCSEC).

Este libro establece los requerimientos para evaluar la efectividad de los controles de seguridad en cómputo incorporados en un sistema. El TCSEC fue usado para evaluar, clasificar y seleccionar sistemas computacionales usados para el procesamiento, almacenamiento y recuperación de información sensitiva o clasificada.

El Orange Book crea 4 divisiones (A, B, C, D) y en cada división crea diferentes clases que sirven para representar la diferencia en la confianza que se les puede tener a los sistemas de una empresa [4]. Las características de las diferentes clasificaciones son las siguientes:

D Esta clasificación está reservada para los sistemas que han sido evaluados pero no cumplen con los requerimientos para estar clasificados en una división más alta.

C1 Esta clasificación cumple con requisitos de seguridad discrecional, es decir, proporcionan una separación de los usuarios con los datos. Los sistemas de esta clasificación incorporan controles capaces de hacer cumplir las limitaciones de acceso.

C2 En esta clasificación los sistemas aseguran el control de acceso de una manera más fina incorporando una revisión de eventos de seguridad y aislamiento de recursos.

B1 Esta clasificación es equivalente al nivel C2 pero cuenta adicionalmente con una declaración informal de una política de seguridad para la clasificación de los datos y el control de acceso obligatorio.

B2 Esta clasificación cubre los requisitos que contienen los sistemas con clasificación B1, sin embargo, los mecanismos de autenticación deben ser reforzados. Los sistemas B2 también deben estar diseñados para ser resistentes al acceso de personas no autorizadas.

B3 Los sistemas B3 a parte de contar con las características de los sistemas de las anteriores clasificaciones, deben monitorear todos los accesos de objetos y sujetos con la finalidad de poder ser analizados más adelante. Los sistemas deben estar diseñados para ser altamente resistentes a la entrada de personas no autorizadas.

A1 Protección verificada. En la práctica es lo mismo que el nivel B3, pues no se agregan políticas, requerimientos u otras funciones adicionales, la diferencia yace en que la seguridad debe estar definida en la fase de análisis del sistema.

Es importante contemplar qué características son las que se necesitan que cubra un sistema y verificar que el sistema cubre con dichas características antes de adquirirlo o desarrollarlo.

3.1.5 FIPS

Federal Information Processing Standards (FIPS) son estándares públicos desarrollados por el gobierno de los Estados Unidos para su uso en las distintas agencias de gobierno.

Entre las publicaciones emitidas por el NIST se encuentran aquellas que contienen los estándares públicos para el cifrado de los datos, tales como *Data Encryption Standard* (DES) o *Advanced Encryption Standard* (AES), aunque también existen estándares de algoritmos no públicos de cifrado como *Escrowed Encryption Standard* (EES); sin embargo, de este tipo de estándares, al contener información clasificada, sólo son mencionados mas no descritos [5]. De los FIPS más importantes se encuentra el FIPS 200, el cual establece los requerimientos mínimos de seguridad, el cual se describe a continuación.

3.1.5.1 FIPS 200

De las diferentes publicaciones de FIPS, el FIPS 200 habla de los requerimientos mínimos de seguridad, estos requerimientos cubren 17 áreas relacionadas con la seguridad [6].

Las 17 áreas son:

Control de Accesos. Las organizaciones deben limitar el acceso a los sistemas de información a los usuarios, procesos o dispositivos y a los tipos de transacciones y funciones que usuarios autorizados tienen permitido ejecutar.

Capacitación y Concientización. Las organizaciones deberán asegurar que los administradores y usuarios de los sistemas de información de la organización conozcan los riesgos de seguridad asociados a sus actividades, así como las leyes aplicables, políticas, estándares, regulaciones o procedimientos relacionados a la seguridad de los sistemas de información de la organización y asegurar que el personal de la organización sea adecuadamente capacitado de acuerdo a sus responsabilidades.

Auditoria y Rendición de Cuentas. Las organizaciones deberán crear, proteger y retener resultados de auditorías de los sistemas de información para permitir el monitoreo, análisis, investigación y reporte de actividad no permitida sobre los sistemas de información, así mismo deberán de asegurar que las acciones de los usuarios de los sistemas de información puedan ser solamente realizados por esos usuarios de manera que sólo a ellos se les puede imponer la responsabilidad de sus acciones.

Certificación, Acreditación y Evaluación de la Seguridad. Las organizaciones deberán evaluar periódicamente los controles de seguridad en los sistemas de información de la organización para determinar si los controles son efectivos en el momento de aplicarlos, también se deberán desarrollar e implementar planes de acción designados para corregir deficiencias y reducir las vulnerabilidades de los sistemas, deberán autorizar la operación de los sistemas de información y cualquier conexión asociada a los sistemas.

Administración de la Configuración. Las organizaciones deberán establecer y mantener una guía de configuraciones e inventario del sistema de información de la organización a través de los respectivos ciclos de vida del desarrollo del sistema, así también, establecer y fortalecer los ajustes de configuración de seguridad para la información de productos de tecnología empleados en los sistemas de información de la organización.

Planes de Contingencia. Las organizaciones deben establecer, mantener e implementar efectivamente planes de respuesta a emergencias, operaciones de respaldo, y de recuperación de desastres para asegurar la disponibilidad de la información y la continuidad de las operaciones en situaciones de emergencia.

Identificación y Autenticación. Las organizaciones deberán identificar a los usuarios de los sistemas de información, los procesos que son ejecutados por los usuarios o dispositivos, y autenticar las identidades de dichos usuarios, procesos o dispositivos como prerrequisito para permitir el acceso a los sistemas de información de la empresa.

Respuesta a Incidentes. Las organizaciones deberán establecer una capacidad de manejo operacional de incidentes para los sistemas de información organizacionales, lo cual incluye una adecuada preparación, detección, análisis, contención, recuperación y respuesta a las actividades de los usuarios, así como también se deberá rastrear, documentar y reportar los incidentes a los funcionarios de la organización y/o autoridades pertinentes.

Mantenimiento. Las organizaciones deberán realizar periódica y oportunamente el mantenimiento sobre los sistemas de información de la organización y proveer controles en las herramientas, técnicas, mecanismos y personas usados para realizar el mantenimiento de los sistemas.

Protección de Medios de Comunicación. Las organizaciones deberán proteger los medios de los sistemas de información, tanto en papeles como en medios electrónicos, limitar el acceso a la información en los medios de los sistemas de información a los usuarios autorizados y sanitizar dichos medios antes de que sean reutilizados o destruirlos si llegase a ser necesario.

Protección Física y Ambiental. Las organizaciones deberán limitar el acceso físico a los sistemas de información, equipo, y a los respectivos ambientes operativos a individuos autorizados, proteger las instalaciones y soporte de la infraestructura para los sistemas, proporcionar utilidades de apoyo para los sistemas de información, proteger los sistemas de información de amenazas ambientales y proporcionar controles ambientales en las instalaciones que contienen a los sistemas de información.

Planeación. Las organizaciones deberán desarrollar, documentar, periódicamente actualizar, e implementar planes de seguridad para los sistemas de información de la organización que describan los controles de seguridad en el lugar planeado para el sistema de información y las reglas de comportamiento para las personas que tienen acceso a los sistemas de información.

Seguridad del personal. Las organizaciones deberán asegurarse que las personas que ocupan puestos de responsabilidad con las organizaciones, incluyendo personal de terceros, son personas de confianza y conocen el criterio de seguridad establecido para esos puestos. También habrá que asegurarse que la información de la organización y de los sistemas es protegida durante y después de las acciones del personal, tales como transferencias y emplear sanciones para el personal que incumpla con las políticas de seguridad de la organización.

Evaluación de Riesgos. Las organizaciones deberán evaluar periódicamente el riesgo de las operaciones de la organización, los activos de la empresa y las personas.

Adquisición de Sistemas y Servicios. Las organizaciones deberán asignar los recursos suficientes para proteger los sistemas de información de la organización, emplear los procesos de ciclo de vida de desarrollo de sistemas que incorporen consideraciones de seguridad de la información, emplear restricciones para el uso e instalación de software y asegurar que los proveedores o terceras personas emplean las medidas de seguridad adecuadas para proteger la información, aplicaciones y servicios externos a la empresa.

Protección del Sistema y Comunicaciones. Las organizaciones deberán monitorear, controlar y proteger las comunicaciones de la organización en los límites externos y los límites internos clave de los sistemas de información, emplear diseños de arquitectura, técnicas de desarrollo de software, y principios de ingeniería de sistemas que promuevan la seguridad de la información con los sistemas de información de la organización.

Integridad del Sistema y de la Información. Las organizaciones deberán identificar, reportar y corregir información y defectos del sistema de información de manera oportuna, se deberá proporcionar protección contra código malicioso en posiciones adecuadas de los sistemas de información y finalmente monitorear las alertas de seguridad de los sistemas de información y tomar las medidas adecuadas en respuesta.

3.2 Controles

Los controles son medidas o salvaguardas implementados para reducir los riesgos de Seguridad Informática.

Hay diferentes clasificaciones para los controles e incluso un mismo control puede ser clasificado de diferentes maneras. Una de las clasificaciones más comunes es por el momento en que actúan, es decir:

- Controles Preventivos: son acciones tomadas para administrar el desarrollo, mantenimiento y uso del sistema, incluyendo políticas específicas de un sistema, así como decisiones de personal de seguridad. Un ejemplo de este tipo de controles son programas de concientización y manejo de control de cambios.
- Controles Detectivos: Son acciones tomadas para detectar eventos no deseados una vez que ya han ocurrido. Ejemplos de este tipo de controles son detectores de intrusos, analizadores de bitácoras, reportes de violación.
- Controles Correctivos: Son acciones tomadas para ayudar a mitigar el impacto de un incidente, suelen ser llamados también controles de recuperación. Ejemplos de este tipo de controles son acciones de contingencia, manejo de respaldos, etc.

Otra clasificación también válida de los controles son los controles operativos, los cuales contemplan procedimientos para proteger la operación diaria de los sistemas. Este tipo de controles se puede clasificar en:

- Controles de Hardware: Contemplan los controles necesarios para proteger el equipo de cómputo durante la operación y mantenimiento del mismo.
- Controles de Software: Contempla los controles necesarios para poder saber cuál es el software que está ejecutando el hardware.
- Controles de Privilegios: Contempla los controles necesarios para operar los sistemas en modo privilegiado o también llamado supervisor.
- Control de Medios: Contempla los controles necesarios para proteger los medios que almacenan a la información.
- Control de Acceso Físico: Contempla los controles necesarios para garantizar el acceso autorizado a los medios y equipos que almacenan la información.

Cuando se haya encontrado alguna vulnerabilidad que puede llegar a ser explotada es importante seleccionar el control adecuado, no obstante hay que recordar que la seguridad tiene un efecto en las actividades de la empresa, por lo cual no hay que caer en el error de usar controles de más intentando de esta manera controlar más amenazas de las que pudieran llegar a existir.

En éste capítulo se han mencionado diferentes estándares de seguridad, algunos de estos estándares mencionan la necesidad de realizar un Análisis de Riesgos, dicho análisis es

importante debido a que, como se vio en el Capítulo 2, el Análisis de Riesgos es uno de los primeros pasos que se siguen para poder implementar la seguridad de la información en alguna organización. En el siguiente capítulo se explicará el proceso de la Administración de Riesgos y cómo es que se relaciona con el Análisis de Riesgos y otras etapas de dicho proceso.

Referencias Capítulo 3

1 ISO/IEC 17799 **“Information Technology – Code of practice for information security management”.** Primera Edición. Estándar publicado por International Organization for Standardization en Suiza en el año-2000.

2 ISO/IEC 27001:2005 “**Information Technology – Security techniques – Information Security Management Systems - Requeriments”.** Primera Edición. Estándar publicado por International Organization for Standardization en Suiza en el año 2005.

3 ISO 7498-2 **“Information processing systems - Open Systems Interconnection - Basic Reference Model Part 2 Security Architecture”.** Primera Edición. Estándar publicado por International Organization for Standardization en Suiza en el año 1989.

4 *United States Government Department of Defense* **“Orange Book”** Primera Edición. Publicado por el Departamento de Defensa de los Estados Unidos en Estados Unidos en el año 1983 Disponible en: http://nsi.org/Library/Compsec/orangebo.txt

5 *NIST* **“Federal Information Processing Standards Publications”.** Pagina Web disponible en: http://www.itl.nist.gov/fipspubs/by-num.htm Leído por última vez el 28 de septiembre de 2009.

6 *FIPS 200* **“Minimum Security Requirements for Federal Information and Information Systems”.** Desarrollado por el NIST. Publicado por el Departamento de Comercio de los Estados Unidos en los Estados Unidos en el año 2006. Disponible en:
http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf

7 Wikipedia The Free Encyclopedia. **“Security Controls”.** Página Web disponible en: http://en.wikipedia.org/wiki/Security_controls Leído por última vez el 28 de septiembre de 2009.

Capítulo

4

Análisis de Riesgos

Resumen

Una vez que una empresa cobra conciencia del problema que conlleva la Seguridad Informática se encuentra con una de las primeras preguntas: ¿Por dónde iniciar?

Algo importante en seguridad informática es saber qué es lo que se quiere proteger, a dónde es hacia dónde se van dirigir los recursos asignados para la seguridad de la organización, pero más importante aún es conocer a la empresa en sí. Como menciona el libro “El arte de la guerra”, escrito hace más de mil años por Sun Tzu: Si uno no se conoce a sí mismo ni a su enemigo estará en riesgo en cada batalla, si se conoce a sí mismo pero no a su enemigo, correrá riesgo en la mitad de las batallas, si se conoce a sí mismo y a su enemigo se podrán tener cien batallas sin estar en riesgo en ninguna de ellas.

Una forma de conocer a una empresa, organización o institución es estudiando sus objetivos, misión, visión y valores y con base en ello es que se podrá saber cuál es la naturaleza de la empresa, qué es lo que pretende lograr y hacia dónde se dirige.

Cualquier empresa va a estar llena de amenazas y sería incosteable protegerse de todas ellas y mientras que un administrador de seguridad debe de protegerse de todas las vulnerabilidades y ataques, ya sea conocidos o desconocidos, aquel que ataca a un sistema sólo necesita explotar una vulnerabilidad.

El ISO 17799 menciona la importancia de establecer los requerimientos de seguridad y una de las fuentes principales para conseguirlo es la realización de un Análisis de Riesgos. Mediante un Análisis de Riesgos se identifican de forma metódica los riesgos de seguridad, lo cual ayudará a obtener conocimiento a cerca de las amenazas a las que se enfrenta la empresa.

---

4 Análisis de Riesgos

El Análisis de Riesgos va relacionado con el proceso de la Administración de Riesgos, no obstante no deben de ser confundidos, ya que no son lo mismo. El Análisis de Riesgos es el primer paso dentro de la Administración de Riesgos. El Análisis de Riesgos es la **herramienta** de la cual hace uso la Administración de Riesgos para identificar los activos, vulnerabilidades y riesgos [1]. A continuación se describe en qué consiste la Administración de Riesgos, su ciclo de vida y su relación con el Análisis de Riesgos.

4.1 Administración de Riesgos

La Administración de Riesgos es el proceso que permite a los administradores del negocio equilibrar los costos operacionales y económicos de las medidas de protección y conseguir beneficios protegiendo los procesos de negocio que apoyan la misión de la empresa [2].

En el proceso de Administración de Riesgos, se identifica, controla y minimiza el impacto de eventos que podrían poner en peligro la operación de la empresa. El objetivo de este proceso

es reducir el riesgo de alguna actividad a un nivel aceptable y justificar las medidas que se van a tomar con la finalidad de obtener la aprobación de la gerencia.

Al ser la Administración de Riesgos un proceso de negocios, como todo proceso de negocios deberá de tener un ciclo de vida de desarrollo de negocios, Business Development Life Cycle (BDLC), el cual se muestra a continuación [2].

4.1.1 Ciclo de Vida de la Administración de Riesgos

El ciclo de vida de la Administración de Riesgos está dividido en 5 fases que son las siguientes:

Fase de Análisis: En esta fase es donde se realiza el Análisis de Riesgos.

Fase de Diseño: En esta fase se hace una preselección de riesgos, se evalúan los riesgos encontrados en el Análisis de Riesgos, se realiza un análisis de impacto al negocio donde se identifica cuánto es lo que le cuesta a la empresa que se materialice un riesgo y se hace una clasificación de la información.

Fase de Construcción: En esta fase se hace la implementación de salvaguardas o controles para las amenazas y se estructura un adecuado control de accesos.

Fase de Prueba: En esta fase se realizan pruebas de las salvaguardas implementadas con la finalidad de verificar que los riesgos identificados han sido reducidos a un nivel aceptable y se inicia un Plan de Continuidad del Negocio.

Fase de Mantenimiento: En esta fase se vuelven a examinar los controles o salvaguardas debido a los cambios o actualizaciones que seguramente ocurrirán, se hace una revisión anual del Plan de Continuidad del Negocio, se revisa el funcionamiento del control de accesos y se hace una evaluación de vulnerabilidades.

La Figura 4.1 muestra las diferentes etapas del Ciclo de Vida de la Administración de Riesgos:

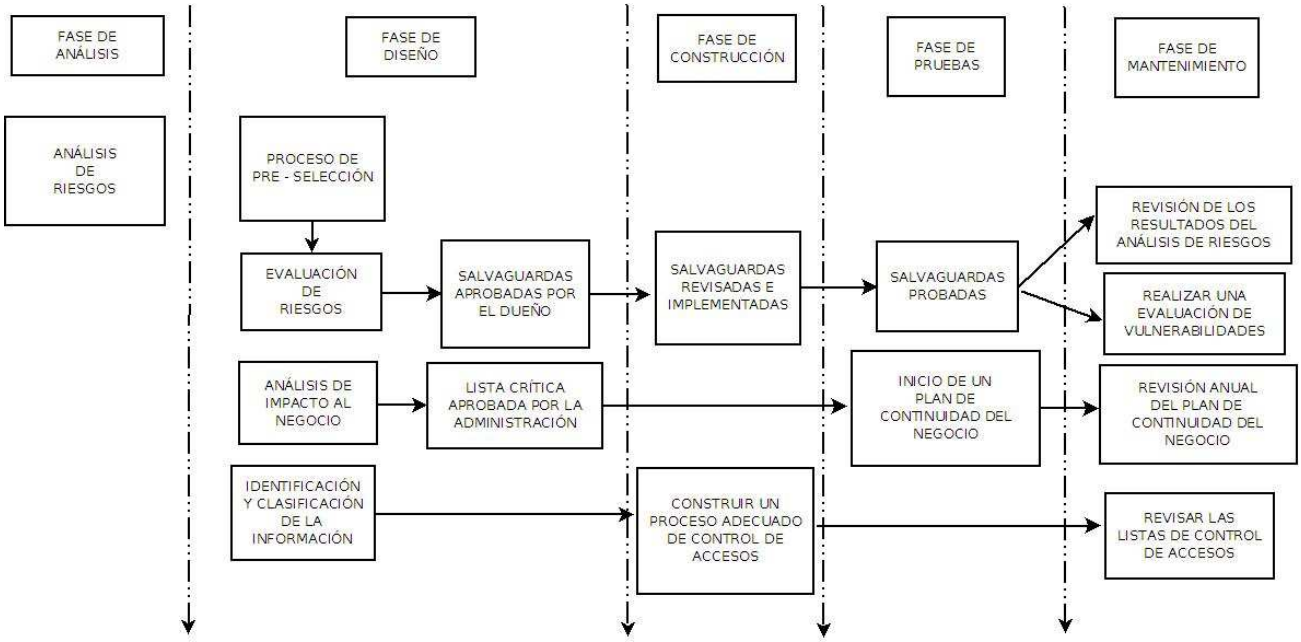


Figura 4.1 Fases del Ciclo de Vida de la Administración de Riesgos

Como se puede observar en la Figura 4.1, el Análisis de Riesgos se encuentra en la primera fase del ciclo de la Administración de Riesgos, esto hace que el Análisis de Riesgos tenga un papel importante para la Seguridad Informática, por lo cual se describe a continuación.

4.1.2 Análisis de Riesgos

El Análisis de Riesgos es una técnica usada para identificar y evaluar factores que pueden poner en peligro la meta de un proyecto o que una empresa pueda alcanzar un objetivo. Permite ayudar a los directivos de negocio a obtener un entendimiento de los riesgos y las vulnerabilidades asociadas a la información y la tecnología que la habilita, y a partir de ello se puede establecer una arquitectura de seguridad que reduzca el nivel de riesgo a grados de impacto que la organización pueda soportar. Para realizar un Análisis de Riesgos, es necesario hacer un análisis costo-beneficio en el que se incluyan las características de los activos y su razón de ser para la empresa, junto con los procesos que se van a evaluar.

Para poder identificar los activos de la empresa e identificar las posibles amenazas para esos activos se requiere de la colaboración de diferentes perfiles dentro de la organización, los cuales van desde perfiles gerenciales, administrativos, e incluso técnicos, ya que las personas que poseen estos perfiles son quienes conocen mejor al sistema, las aplicaciones y a la empresa, debido a que son ellos quienes interactúan en la empresa diariamente, por ello es necesario aprovechar los conocimientos de estas personas ya que quien conoce mejor a la empresa son las personas que laboran en ella y que una persona externa difícilmente puede terminar de conocer. Contar con el apoyo de la gerencia es necesario ya que se necesita que todos los involucrados en el Análisis de Riesgos tengan claro que es importante su participación.

El Análisis de Riesgos puede hacerse antes de tomar medidas de seguridad o después, no obstante es recomendable hacerlo antes, ya que en caso de que no se tomen las medidas adecuadas de seguridad con anticipación, corregirlas después será costoso en tiempo y

dinero, en cambio, hacerlo antes permite anticiparse a diferentes sucesos y llegar a tener un buen grado de eficiencia.

El primer paso para realizar el Análisis de Riesgos es definir los activos que van a ser revisados. En este paso se define la aplicación, el sistema o la amenaza que se va a revisar. También es importante definir los límites de lo que va a ser revisado, esto debe de ser realizado con cuidado pues si no se realiza correctamente el Análisis se saldrá de control. Es preferible involucrar en este paso al dueño de la empresa pues él puede indicar que activos de la empresa le parecen más relevantes.

El segundo paso es Identificar las Amenazas que afectan a los activos. Como ya se vio en el capítulo 1, una amenaza es un evento no deseado que puede tener un impacto negativo en los objetivos del negocio o en su misión. El origen de una amenaza está definido como cualquier circunstancia o evento con el potencial de causar daño al activo en revisión. Existen diferentes orígenes para las amenazas, una amenaza puede deberse a que se implementan controles de forma incorrecta o han dejado de ser útiles y ahora representan una vulnerabilidad que puede ser explotada. En este paso se deberá hacer una lista de los orígenes de las amenazas tan completa como sea posible.

Para crear una lista de amenazas existen diferentes métodos que pueden ser utilizados, entre ellos se incluye el desarrollo de listas de verificación, las cuales se basan en el flujo de ideas e información. Otra forma de obtener las amenazas es buscar qué eventos han ocurrido en el pasado a la organización y con qué frecuencia. Una vez obtenida la amenaza será necesario obtener su *Annual Rate of Ocurrance* (ARO). Otro método que también puede ser usado y que también puede resultar muy útil es la lluvia de ideas.

Los resultados de un Análisis de Riesgos ayudarán a determinar la acción apropiada y las prioridades para manejar los riesgos de seguridad de la información e implementar los controles para esos riesgos.

4.1.3 Evaluación de Riesgos

La Evaluación de Riesgos consiste en determinar las amenazas que existen para un activo en específico y el nivel de riesgo asociado a dichas amenazas. Realizar una priorización de amenazas es lo que permite a la empresa seleccionar los controles adecuados para reducir la amenaza a un nivel aceptable.

Para realizar la Evaluación de Riesgos, el primer paso consiste en determinar la probabilidad de ocurrencia.

Una vez que se ha obtenido la lista de amenazas, será necesario determinar que tan a menudo se presentan. Dependiendo del enfoque del análisis que se esté usando, será la forma de determinar las probabilidades, por ejemplo, en un Análisis de Riesgos cualitativo, se pueden establecer las probabilidades en:

- Alta: Esta probabilidad se presenta cuando es casi un hecho que una amenaza se va

a materializar.
- Media: Indica que posiblemente una amenaza se materializará.
- Baja: Muy poca probabilidad de que la amenaza se materialice.

El siguiente paso será determinar el impacto de la amenaza. Una vez determinada la probabilidad de ocurrencia de la amenaza, será necesario determinar el impacto que la amenaza tendrá en la organización. En un Análisis de Riesgos realizado desde un enfoque cualitativo, los impactos de las amenazas pueden clasificarse de la siguiente manera:

- Impacto Alto: Cierre de la unidad de negocio que conduce a una pérdida significativa para el negocio, a la imagen corporativa o a las ganancias de la empresa

- Impacto Medio: Pequeña interrupción de procesos o sistemas críticos que resulta en una pérdida financiera limitada.

- Impacto Bajo: Interrupción que no origina ninguna pérdida.

Después de haber establecido el nivel del impacto de las amenazas, el siguiente paso será determinar los controles que pueden ser usados para reducir las amenazas. Es importante identificar los controles que pueden reducir el riesgo a un nivel aceptable, para ello es necesario saber que tan efectivo puede ser el control que se va a escoger, tomando en cuenta la probabilidad de ocurrencia y el nivel de impacto de la amenaza con el control puesto. Si el nivel de riesgo no se reduce a un nivel aceptable, entonces será necesario evaluar algún otro control.

Es muy común encontrar con que diferentes autores confunden lo que es el Análisis de Riesgos con la Evaluación de riesgos. Hay que entender que durante el Análisis de Riesgos se identifican las amenazas a los activos y en la Evaluación de Riesgos se evalúan las amenazas encontradas en el Análisis de Riesgos.

4.1.4 Mitigación de Riesgos

La mitigación de riesgos es una técnica para reducir los riesgos de la empresa una vez que estos han sido evaluados. Después de conocer los riesgos, la administración puede utilizar diferentes métodos de mitigación para completar el proceso. Los 5 métodos más comunes de mitigación de riesgos son:

- Aceptar el riesgo.
- Mitigar el riesgo.
- Evitar el riesgo.
- Planear el riesgo.
- Transferir el riesgo.

Un riesgo se puede aceptar cuando después de evaluar las amenazas y su nivel de riesgo, éstas no representan una gran amenaza para la producción del negocio y su impacto es bajo, aunque hay ocasiones en que se acepta debido a que el costo de mitigar ese riesgo es tan alto que no es efectivo en costo para la organización.

Mitigar el riesgo consiste en poner los controles que eviten o minimicen el impacto de un riesgo a un nivel aceptable.

Evitar el riesgo es no tomar acciones que podrían hacer que el riesgo se materialice, por ejemplo, una organización puede usar los servicios de la banca electrónica, pero analizando los fraudes que se llegan a cometer en las transacciones electrónicas, puede tomar la decisión de evitar el riesgo de un fraude y optar por seguir realizando sus pagos acudiendo físicamente a la sucursal de un banco.

Planear el riesgo es un proceso donde se decide manejar el riesgo desarrollando una arquitectura que prioriza, implementa y mantiene controles.

La opción de transferir el riesgo consiste en hacer que alguna persona externa a la organización se encargue de mitigar los riesgos. Un ejemplo de esto es cuando las empresas contratan consultorías o servicios de *out sourcing*. Hay que tener cuidado cuando se escoge esta alternativa ya que así como una empresa puede tener problemas internos con sus empleados, una empresa externa que se llegue a contratar puede tener los mismos problemas, lo cual no garantiza que esta opción sea la mejor.

Sin importar el método que se utilice para mitigar los riesgos, es necesario considerar siempre los objetivos de la empresa o la misión cuando se va a seleccionar un método.

Como se vio en el Capítulo 2, la seguridad informática tiene un ciclo, y éste se repite constantemente, esto implica que el Análisis de Riesgos se deberá repetir periódicamente para contemplar cualquier cambio que pudiese influir en los resultados del Análisis de Riesgos.

4.2 Enfoques del Análisis de Riesgos

Para realizar el Análisis de Riesgos existen dos enfoques: existe el enfoque Cuantitativo y el enfoque Cualitativo. Cada enfoque posee sus ventajas con sus respectivas desventajas que deberán de ser tomadas en cuenta al momento de seleccionar que enfoque es el que se va a utilizar.

4.2.1 Enfoque Cuantitativo

Un enfoque Cuantitativo asigna números reales a los elementos del riesgo, es decir, se obtienen valoraciones numéricas absolutas sobre los activos y los riesgos. Su principal ventaja es que hacer operaciones con valores numéricos es algo natural y arroja resultados claros, no obstante, este tipo de enfoque puede resultar poco práctico ya que al momento de realizar cálculos matemáticos se debe tener la certeza de que los datos usados realmente son correctos ya que en cualquier ecuación matemática no es desconocido que si un solo valor es incorrecto, el resultado no puede ser correcto.

En la Tabla 4.1 se muestran las ventajas y desventajas de realizar el Análisis de Riesgos bajo

un enfoque Cuantitativo:

Análisis Cuantitativo	
Ventajas	Desventajas
Es un proceso objetivo que establece métricas	Los cálculos son complejos
Ayuda para poder establecer mas expresivamente una relación costo-beneficio	Es necesario una gran cantidad de trabajo preliminar
Al ofrecer los resultados de forma numérica, es más fácil de comprender en un lenguaje administrativo	Es difícil manejar resultados que no están dentro del objetivo
	No es fácil capacitar al personal que se involucrará a través del proceso

Tabla 4.1 Ventajas y Desventajas del Análisis Cuantitativo

4.2.2 Enfoque Cualitativo

En un Análisis de Riesgos realizado con un enfoque Cualitativo, se deberán de establecer las probabilidades de que ocurra alguna amenaza, el impacto en caso de que se materialice la amenaza, y que tan bien están funcionando las salvaguardas o contramedidas para reducir el riesgo a un nivel aceptable. Este enfoque no asigna valores numéricos ni monetarios, en vez de decir cuánto vale un riesgo, dice si el riesgo es Alto, Medio o Bajo. Al no buscar valores numéricos permite avanzar más rápido ya que se posiciona el valor de cada activo en un orden relativo respecto de los demás. La limitación de este enfoque es que no permite sumar valores más allá de su orden relativo.

En la Tabla 4.2 se muestran las ventajas y desventajas de realizar el Análisis de Riesgos bajo un enfoque Cuantitativo:

Análisis Cualitativo	
Ventajas	Desventajas
Los cálculos son simples	Es de naturaleza subjetiva
No es necesario asignar un valor monetario a un activo	No ayuda a realizar un análisis costo-beneficio
Es flexible en el proceso y en los resultados	No se obtiene el valor monetario de los activos
Es fácil involucrar personal que no sea del área de seguridad ni de alguna área técnica	

Tabla 4.2 Ventajas y Desventajas del Análisis Cualitativo

Una vez que se haya terminado de realizar el Análisis de Riesgos dentro de una empresa, las amenazas y vulnerabilidades seguirán existiendo, en otras palabras la empresa estará igual que al principio pero con la ventaja de que ahora tendrá conocimiento de qué es lo que puede impedir que la empresa cumpla con su misión y sus objetivos. El conocimiento de las vulnerabilidades de una empresa, del riesgo de que se materialice una amenaza y de los procesos críticos de la empresa, es lo que le da a la empresa la oportunidad de poder actuar de manera preventiva.

Cualquier empresa que decida realizar un Análisis de Riesgos, para su eficiencia deberá de seguir alguna metodología. Por lo general las distintas metodologías presentan una serie de pasos similares, no obstante, existen diferencias que deben ser tomadas en cuenta al momento de elegir la metodología con la cual se realizará el Análisis. En el siguiente capítulo se describen diferentes metodologías con las cuales se puede realizar un Análisis de Riesgos y se explicarán las diferencias entre todas ellas.

Referencias Capítulo 4

1 *Francisco López Crespo, Miguel Angel Amutio Gómez, Javier Candau, José Antonio Mañas.* **"Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información".** Versión 2. Metodología publicada por el MINISTERIO DE ADMINISTRACIONES PÚBLICAS En España en el año 2006 Disponible en: http://www.csae.map.es/csi/pdf/magerit_v2/metodo_v11_final.pdf

2 *Thomas R. Peltier* **"Information Security Risk Analysis".** Ed. Auerbach Publications. Segunda Edición. Publicado en Estados Unidos en el año 2005.

Capítulo 5

Metodologías para el Análisis de Riesgos: Un Análisis Comparativo

Resumen

Realizar un Análisis de Riesgos no es una labor sencilla, es un proceso complejo, y para realizarlo de manera ordenada existen diferentes metodologías, cada una de ellas cuenta más o menos con los mismos procedimientos, es decir, identificar los principales activos, las amenazas que enfrentan dichos activos, el riesgo de que se presente una amenaza, el costo a la organización si la amenaza se materializa, y los posibles controles para mitigar el riesgo, no obstante hay diferencias significativas entre ellas.

En este capítulo se describen algunas de las metodologías más comunes para la realización del Análisis de Riesgos. Estas metodologías han sido desarrolladas por diferentes organismos, y aunque tienen la misma finalidad y pasos similares es conveniente conocerlas para saber cuál es la que conviene usar en diferentes situaciones, ya que de acuerdo a las circunstancias en que se encuentre la empresa puede resultar más conveniente usar una metodología u otra.

---

5 Metodologías para el Análisis de Riesgos: Un Análisis Comparativo

A continuación se describen diferentes Metodologías para la realización del Análisis de Riesgos.

5.1 OCTAVE

Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) es una Metodología para realizar Análisis de Riesgos, la cual está desarrollada por CERT® *Coordination Center*, el cual forma parte del *Software Engineering Institute* (SEI) que es operado por la Universidad *Carnegie Mellon* en Pittsburg Pensilvania en nombre del Departamento de Defensa de los Estados Unidos [1].

OCTAVE es una metodología para la búsqueda de la seguridad informática basada en el análisis estratégico del riesgo y la planeación de una técnica para su implementación. Esta metodología está integrada por un compendio de criterios que definen los elementos esenciales para un Análisis y Evaluación de Riesgos de seguridad informática.

CERT ha creado diferentes versiones de OCTAVE, actualmente en su página se encuentran:

- OCTAVE Method desarrollado para empresas de 300 empleados o más.
- OCTAVE-S desarrollado para empresas de 100 empleados o menos.
- OCTAVE-Allegro es una variante de OCTAVE Method pero enfocado a los activos de información.

Estas tres metodologías pueden bajarse gratuitamente de la página de CERT®

OCTAVE tiene por objetivo que las organizaciones sean capaces de:

- Dirigir y administrar un Análisis de Riesgos por sí mismas.
- Tomar las mejores decisiones basándose en el conocimiento de sus propios riesgos.
- Enfocarse en proteger la información más sensitiva.
- Comunicar de manera segura la información sensitiva de la empresa.

OCTAVE Method está contenido en 12 volúmenes y consta de tres fases, cada fase cuenta con sus respectivos procesos llegando a tener 8 procesos en total. OCTAVE contempla diferentes actividades previas a la realización del Análisis de Riesgos, estas actividades incluyen la selección de un equipo con diferentes personas de las diversas áreas de la empresa, este equipo deberá ser capacitado para poder realizar el Análisis, así mismo se deberá de hacer una planeación cuidadosa para aplicar la metodología y hacer el Análisis correctamente.

Las fases para realizar el Análisis de Riesgos bajo esta metodología se describen a continuación:

Fase 1

La primera fase está dividida en cuatro procesos y tiene como objetivo determinar cuáles son los activos informáticos críticos para la operación de la empresa e identificar que se hace actualmente para protegerlos.

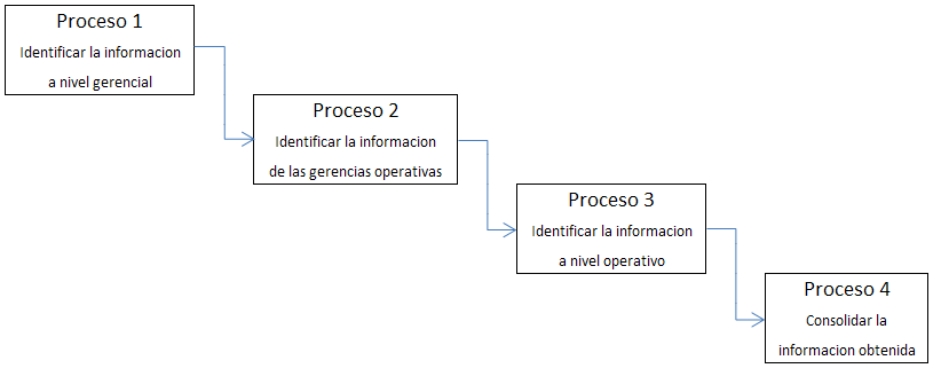


Figura 5.1 Primera Fase de la Metodología OCTAVE

Como se puede observar en la Figura 5.1, los Procesos 1, 2 y 3 tienen como objetivo el obtener información desde diferentes puntos de vista dentro de la empresa, los cuales van desde el nivel gerencial hasta el nivel operativo. Una vez reunida la información, ésta se consolidará en el Proceso 4, de esta manera se obtendrán los requerimientos de seguridad junto con la medidas que se están llevando a cabo justo antes de realizar el Análisis de Riesgos.

Fase 2

La segunda fase consiste en identificar las vulnerabilidades de la infraestructura informática

en cuanto a:

- Red.
- Arquitectura.
- Sistema Operativo.
- Aplicaciones.

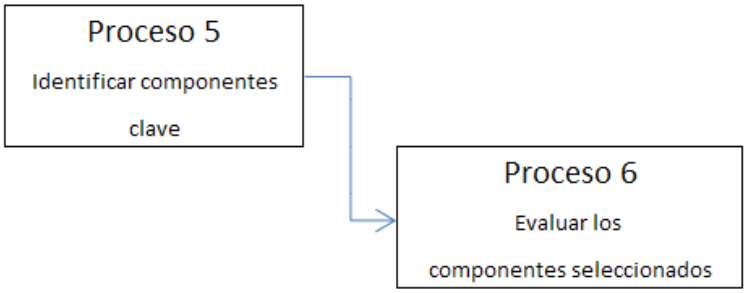


Figura 5.2 Segunda Fase de la Metodología OCTAVE

De acuerdo con la figura 5.2, en el Proceso 5 se evaluarán los sistemas más importantes con la finalidad de identificar los activos cuyo valor sea importante para la empresa. En el Proceso 6 se evaluarán los componentes seleccionados para poder obtener las vulnerabilidades de los activos importantes.

Fase 3

La tercera fase está dividida en dos procesos, dentro de los cuales se desarrollan planes y estrategias de seguridad para soportar la misión y las prioridades de la empresa.

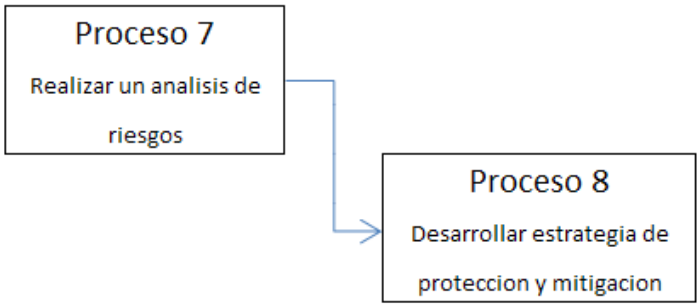


Figura 5.3 Tercera Fase de la Metodología OCTAVE

La Figura 5.3 muestra la última fase de esta metodología. En el Proceso 7 se realizará un Análisis de Riesgos sobre los activos críticos de la empresa, en el Proceso 8 se propondrán acciones, planes y estrategias con la finalidad de poder proteger los activos de la empresa.

En la implementación se incorporan planes y estrategias en las políticas de la empresa, se mantiene un grupo de evaluación y seguimiento continuo, se permiten revisiones que adopten nuevas formas de seguridad.

Los resultados del método OCTAVE se ilustran en la Figura 5.4.

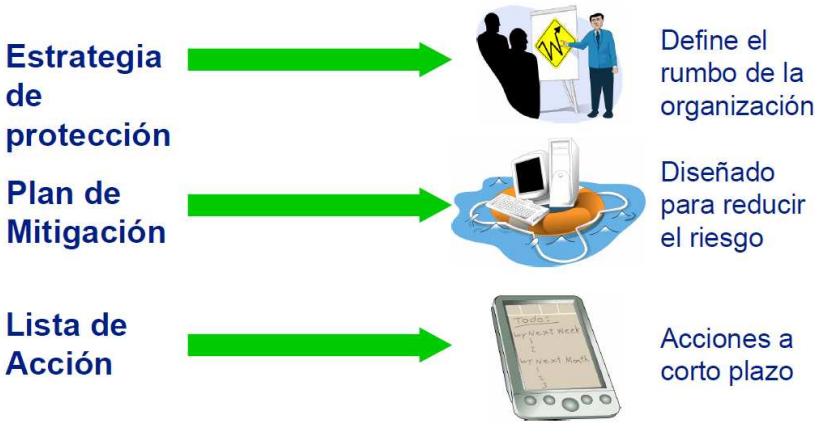


Figura 5.4 Salidas de la Metodología OCTAVE

La Figura 5.4 muestra los resultados que debe de arrojar el Análisis realizado con la metodología OCTAVE. Al haber realizado la metodología OCTAVE se deberá de obtener una Estrategia de Protección, un Plan de Mitigación diseñado para reducir los riesgos y una Lista de Acciones a corto plazo. Todos estos resultados deberán de ir alineados a los objetivos de la empresa.

Aunque el proceso de Análisis de Riesgos con OCTAVE por sí mismo es interesante, en los volúmenes que integran a la metodología se encuentran diferentes escenarios de ejemplo, los cuales facilitarán llevar a cabo el Análisis, lo cual le da un valor extra a esta metodología.

5.2 MAGERIT

MAGERIT es una metodología de carácter público perteneciente al Ministerio de Administraciones Públicas de España. Su utilización no requiere de una autorización previa [2].

Hasta la fecha han salido dos versiones de esta metodología, la primera surgió en 1997 y la segunda versión surgió en el año 2004.

Esta metodología se enfoca al Análisis de Riesgos cuantitativo, pues se considera que es más fácil trabajar con cifras numéricas con las que se pueden realizar operaciones matemáticas que con estimaciones relativas.

MGERIT no sólo se enfoca al Análisis de Riesgos, también abarca el tema de la Administración de Riesgos.

La Administración de Riesgos permite organizar la defensa concienzuda y prudente, defendiendo para que no pase nada malo, y a la vez estar preparados para atajar las emergencias, sobrevivir a los incidentes y seguir operando en las mejores condiciones.

MAGERIT tiene como objetivos:

- Crear conciencia en los responsables de los sistemas de información de la existencia de riesgos y de la necesidad de atajarlos a tiempo.

- Ofrecer un método sistemático para analizar tales riesgos.

- Ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control.

- Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

La metodología MAGERIT realiza el Análisis de Riesgos en cinco pasos que son:

- Paso 1: Determinar los activos relevantes para la empresa, su interrelación y su valor, en el sentido de qué costo supondría su degradación.

- Paso 2: Determinar a qué amenazas están expuestos los activos relevantes para la empresa.

- Paso 3: Determinar qué salvaguardas hay dispuestas y que tan eficaces son frente al riesgo.

- Paso 4: Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.

- Paso 5: Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia o expectativa de materialización de la amenaza.

En el primer paso se identifican los activos con los que se cuenta, no obstante, también se clasifican los activos por su tipo y se encuentran las dependencias que existen entre los activos, es decir, la medida en que un activo superior se vería afectado por un incidente de seguridad en un activo inferior.

En el segundo paso de la metodología se determinan las amenazas que afectan a cada activo. Como se vio en el capítulo 1, una amenaza es cualquier circunstancia con el potencial suficiente para causar perdida o daño al sistema. En este caso interesa lo que puede pasarle a los activos identificados en el primer paso.

MAGERIT estima la vulnerabilidad en dos sentidos: en cuanto a degradación y frecuencia. La degradación mide el daño causado por un incidente en el supuesto de que ocurriese. La frecuencia pone en perspectiva aquella degradación, pues una amenaza puede ser de terribles consecuencias, pero de muy improbable materialización, mientras que otra amenaza puede ser de muy bajas consecuencias, pero tan frecuente como para acabar acumulando un daño considerable.

En el tercer paso se evalúan las salvaguardas o contramedidas que se usan para reducir el riesgo.

La idea de poner una salvaguarda es que deben de evitar el riesgo que pretenden reducir. La salvaguarda ideal es 100% eficaz, lo que implica que:

- es teóricamente idónea.
- está perfectamente desplegada, configurada y mantenida.
- se emplea siempre.
- existen procedimientos claros de uso normal y en caso de incidencias.
- los usuarios están formados y concienciados.
- existen controles que avisan de posibles fallos.

Entre una eficacia del 0% para las salvaguardas que están de adorno y el 100% para aquellas que son perfectas, se estimará un grado de eficacia real en cada caso concreto.

En el cuarto paso se determina el impacto, que viene siendo la medida del daño sobre el activo derivado de la materialización de una amenaza. Conociendo el valor de los activos (en varias dimensiones) y la degradación que causan las amenazas, se puede derivar el impacto que éstas tendrían sobre el sistema. La única consideración que queda hacer es relativa a las dependencias entre activos.

En el quinto paso se determina el riesgo, conociendo el impacto de las amenazas sobre los activos se puede estimar el riesgo teniendo en cuenta la frecuencia de ocurrencia. Las salvaguardas entran en el cálculo del riesgo de dos formas: reduciendo la frecuencia de las amenazas o limitando el daño causado

Una vez que se ha concretado el Análisis de Riesgos MAGERIT a continuación viene la administración de los riesgos encontrados durante el análisis.

Durante la Administración de Riesgos se hace una selección de salvaguardas para atajar el impacto y el riesgo minimizando el daño a los activos como la frecuencia de la amenaza. Es importante saber seleccionar el tipo de salvaguardas que se implementaran haciendo un análisis costo–beneficio para obtener un equilibrio de entre lo que se invierte y lo que se arriesga. No es posible implementar controles para cada riesgo que se encuentre, pero si se puede llegar a cubrir una parte importante reduciendo las pérdidas significativamente.

La decisión sobre qué nivel de impacto y riesgo es aceptable es tomada por la dirección de la organización. Esta decisión no es tomada con fundamentos técnicos sino en base a las necesidades de la empresa las cuales son conocidas por la dirección.

5.3 NIST Publicación Especial 800-30

800-30 es una publicación de NIST. Esta metodología menciona que el objetivo principal del proceso de Administración de Riesgos debería ser proteger a la organización y su habilidad para cumplir con su misión y no tanto los activos de tecnologías de información [3].

800-30 es una guía que puede ser usada por organizaciones no gubernamentales, es pública y no requiere que se paguen derechos por usarla.

El objetivo de NIST 800-30 es que la organización que use esta metodología sea capaz de cumplir con su misión a través de:

- Asegurar los sistemas de información que almacenan, procesan o transmiten información de la organización.

- Permitir a la administración tomar decisiones teniendo un buen conocimiento de los riesgos para justificar los gastos que forman parte del presupuesto de TI.

- Asistir a la gerencia en la autorización o acreditación de sistemas de TI en base a la documentación de soporte resultado del desempeño de la Administración de Riesgos.

Esta metodología realiza el Análisis de Riesgos en 9 pasos los cuales se muestran en la Figura 5.5:

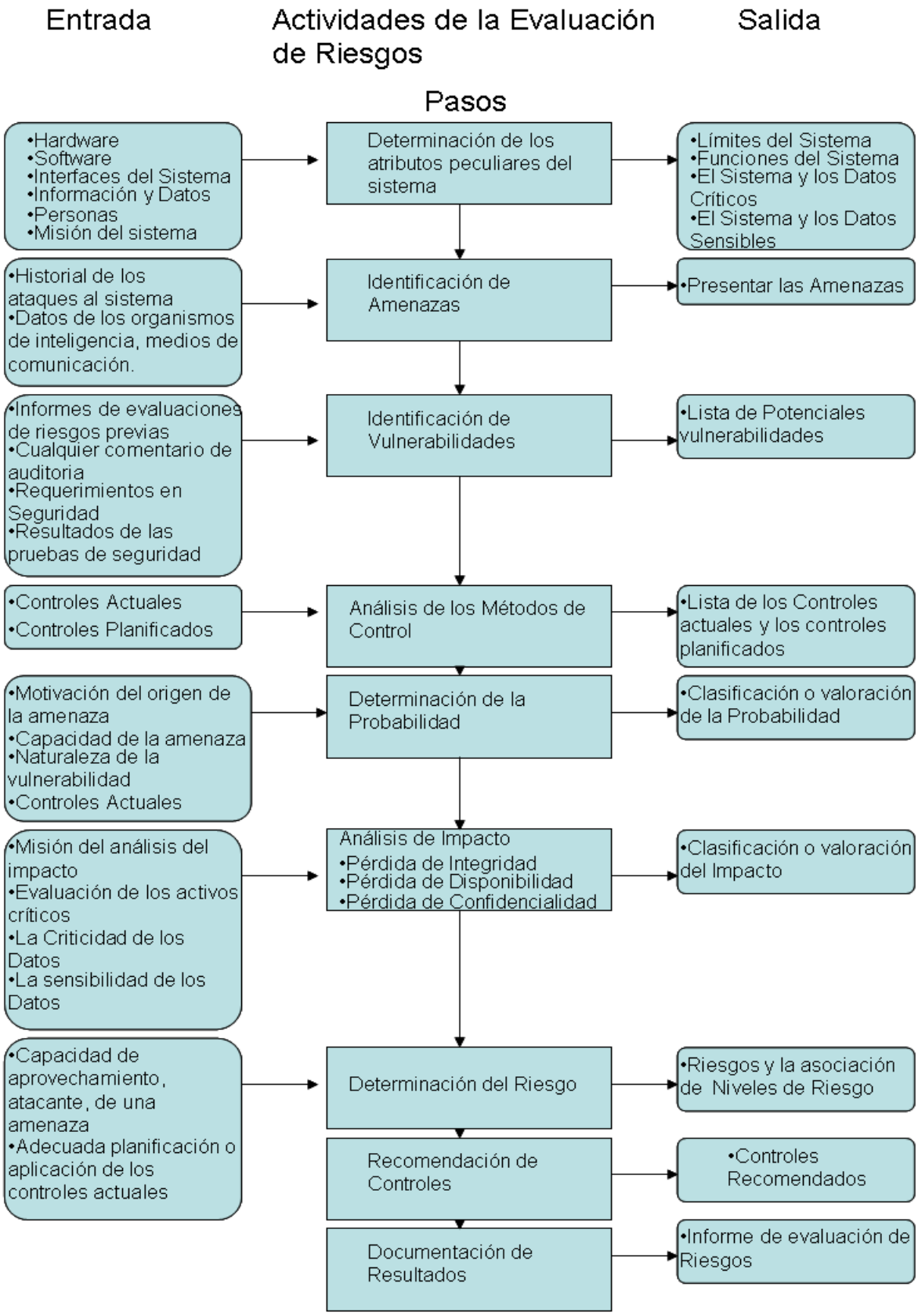


Figura 5.5 Entradas y Salidas de los 9 pasos de la Evaluación de Riesgos propuestas por la Publicación Especial 800-30 del NIST

A continuación se describen los 9 pasos mostrados en la Figura 5.5.

El primer paso consiste en definir el objetivo, definir los límites de los sistemas de información y proveer de información esencial para definir el riesgo.

Para todo ello, este estándar sugiere las siguientes técnicas para obtener información:

- Cuestionarios.
- Entrevistas en sitio.
- Revisión de documentación.
- Uso de herramientas de escaneo automatizadas.

En este paso al finalizar se deberá tener una imagen del ambiente del sistema de información y una delineación del límite del sistema.

El segundo paso consiste en la identificación de amenazas. En este paso se busca identificar el origen de la amenaza que pueda dañar al sistema. Este estándar señala que los orígenes de amenazas más comunes son naturales, humanas, o ambientales. En el caso de las amenazas humanas, éstas necesitan de una motivación para originarse. El estándar da un ejemplo de qué amenazas pueden existir, su origen, su motivación y las acciones que pudiesen realizar en contra de la organización.

En este paso al finalizar se deberá tener una lista con los orígenes de amenazas que pueden explotar vulnerabilidades del sistema

El tercer paso consiste en hacer una lista de las vulnerabilidades del sistema que pudieran ser explotadas por amenazas potenciales. Para identificar las vulnerabilidades tanto técnicas como no técnicas, se pueden usar los métodos descritos en el primer paso, también se pueden consultar sobre vulnerabilidades ya documentadas por la empresa.

En este paso son recomendados realizar pruebas de seguridad al sistema, para hacer dichas pruebas los métodos recomendados son:

- Herramientas automatizadas de escaneo de vulnerabilidades.
- Evaluación y pruebas de seguridad.
- Pruebas de penetración.

Se realiza una lista que contiene estándares básicos de seguridad que pueden ser usados para evaluar e identificar las vulnerabilidades de los activos, procedimientos no automatizados, procesos y transferencias de información asociadas con un sistema de TI en las siguientes áreas:

- Área de Administración.
- Área Operacional.
- Área Técnica.

La salida de este proceso es una lista de requerimientos, y esta lista puede ser usada como entrada para una evaluación de cumplimiento. Este proceso identifica debilidades del sistema, de procesos y procedimientos.

El cuarto paso consiste en un análisis de controles que han sido implementados o se planean implementar para minimizar la probabilidad de que una amenaza explote una vulnerabilidad.

Los controles de seguridad pueden ser métodos técnicos o no técnicos. Los controles técnicos son salvaguardas que se incorporan en los equipos de computo tales como mecanismos de control de acceso, mecanismos de identificación y autenticación, métodos de cifrado, etc. Los controles no técnicos son controles administrativos u operacionales, tales como políticas de seguridad, procedimientos operacionales, seguridad física entre otros.

En este paso, al finalizar se deberá tener una lista de los controles que se están usando o que se planean usar para reducir la probabilidad de que se explote una vulnerabilidad y reducir el impacto de dicho evento.

El quinto paso consiste en realizar una determinación de probabilidades. Para obtener el rango total de probabilidad que indica la probabilidad que una vulnerabilidad potencial puede ser ejecutada se deben considerar los siguientes factores:

- Motivación y capacidad de la amenaza.
- Naturaleza de la vulnerabilidad.
- Existencia y efectividad de los controles que se tengan en ese momento.

La probabilidad de que una vulnerabilidad potencial pueda ser explotada por una amenaza puede ser descrita como alta, media o baja y como salida de este paso se obtiene este rango de probabilidades.

El sexto paso consiste en realizar un análisis de impacto. Se debe determinar el impacto de explotar con éxito una vulnerabilidad. Antes de realizar el análisis de impacto es necesario obtener la siguiente información:

- Misión del sistema.
- Datos críticos del sistema.
- Datos sensitivos del sistema.

Esta información puede obtenerse de la documentación de la organización. Si no existe esta documentación, entonces esa información se puede determinar basándose en el nivel de protección requerida para mantener al sistema y la disponibilidad, integridad y confidencialidad de los datos. Independientemente del método usado para determinar que tan sensitivos son un sistema de TI y los datos, los dueños del sistema y de la información son los únicos responsables de determinar el nivel de impacto para su propio sistema e información. Debido a esto es que un buen comienzo es una entrevista con el dueño del sistema y de la información.

El impacto adverso de un acontecimiento de seguridad puede ser descrito en términos de pérdida o degradación de alguno, o una combinación de alguno, de los tres servicios de

seguridad del Triángulo CIA.

Algunos impactos tangibles pueden ser medidos cuantitativamente, como por ejemplo, en el costo de reparar el sistema, o el nivel de esfuerzo requerido para corregir problemas causados por la acción de una amenaza acertada. Otros impactos, como la pérdida de confianza pública o la pérdida de credibilidad, entre otros, no pueden ser medidos en unidades específicas, pero pueden ser calificados o descritos en términos de alto, medio, o bajo impacto.

Al igual que el Análisis de Riesgos puede hacerse de manera cuantitativa o cualitativa, el análisis de impacto también puede hacerse de ambas formas. En esta metodología se sugiere que se haga de forma cualitativa.

La salida de este paso será una escala en la magnitud del impacto (alto, medio o bajo)

En el séptimo paso se hace una determinación del riesgo. Se determina el nivel de riesgo de los activos para cada amenaza o vulnerabilidad, lo cual se puede expresar en función de:

- La probabilidad de que una amenaza intente explotar una vulnerabilidad.
- La magnitud del impacto cuando una amenaza explotase satisfactoriamente una vulnerabilidad.
- Los controles de seguridad existentes para reducir o eliminar el riesgo.

La salida de este paso consiste en conocer el nivel de riesgo de manera cualitativa, es decir, alto, medio o bajo.

En el octavo paso se hacen las recomendaciones de los controles que pueden mitigar o eliminar los riesgos identificados. El objetivo es reducir el nivel del riesgo a un nivel aceptable.

En este paso es importante saber que no se pueden poner todos los controles para evitar todos los riesgos, hay que hacer una evaluación costo–beneficio para determinar los más apropiados para la organización.

La salida de este paso son las recomendaciones de controles y soluciones alternas para mitigar el riesgo.

El noveno paso consiste en la documentación de los resultados. Una vez que se ha completado el Análisis de Riesgos los resultados se deberán documentar en un informe oficial.

Un informe de Análisis de Riesgos es un informe administrativo que sirve a distintos fines, tales como apoyar la misión de la empresa y a la administración, ayuda en la toma de decisiones con respecto a las políticas, procedimientos y asignación del presupuesto.

A diferencia de una auditoria, en la cual se busca lo que no se está haciendo correctamente, un reporte de Análisis de Riesgos no se debe de presentar de manera acusatoria, debe de ser sistemático y analítico en cuanto a la evaluación del riesgo, de forma que la dirección

entienda los riesgos y asigne recursos para evitar para evitar pérdidas.

La salida de este paso consiste en el reporte del Análisis de Riesgos que describe las amenazas y vulnerabilidades, medidas del riesgo y que provee recomendaciones para la implementación de controles.

Esta metodología cuenta con un segundo proceso para mitigar el riesgo, este proceso involucra la priorización, evaluación e implementación de los controles adecuados para reducir los riesgos encontrados del proceso de Análisis y Evaluación de Riesgos.

La eliminación de riesgos es usualmente impráctica o casi imposible, debido a ello es responsabilidad de los administradores implementar los controles más apropiados para reducir el riesgo a un nivel aceptable con un mínimo impacto adverso a la organización.

En esta metodología se ofrecen las siguientes opciones para mitigar el riesgo:

Asumir el riesgo: consiste en aceptar el riesgo potencial y continuar operando o implementar controles para disminuir el riesgo a un nivel aceptable.

Evadir el riesgo: consiste en evadir el riesgo eliminando o evitando la causa que origina al riesgo.

Limitar el riesgo: consiste en implementar controles que minimizan el impacto adverso de atacar una vulnerabilidad.

Planear el riesgo: consiste en administrar el riesgo desarrollando un plan de mitigación de riesgos que priorice, implemente y mantenga controles.

Transferir el riesgo: consiste en transferir el riesgo usando otras opciones para compensar la pérdida.

De todo esto surgen algunas preguntas: ¿Cuándo y bajo qué circunstancias se debe de tomar acción? ¿Cuándo se implementaran controles para mitigar el riesgo y proteger a la organización?

Para determinar si se puede aceptar un riesgo o no, se puede consultar el siguiente diagrama mostrado en la Figura 5.6:

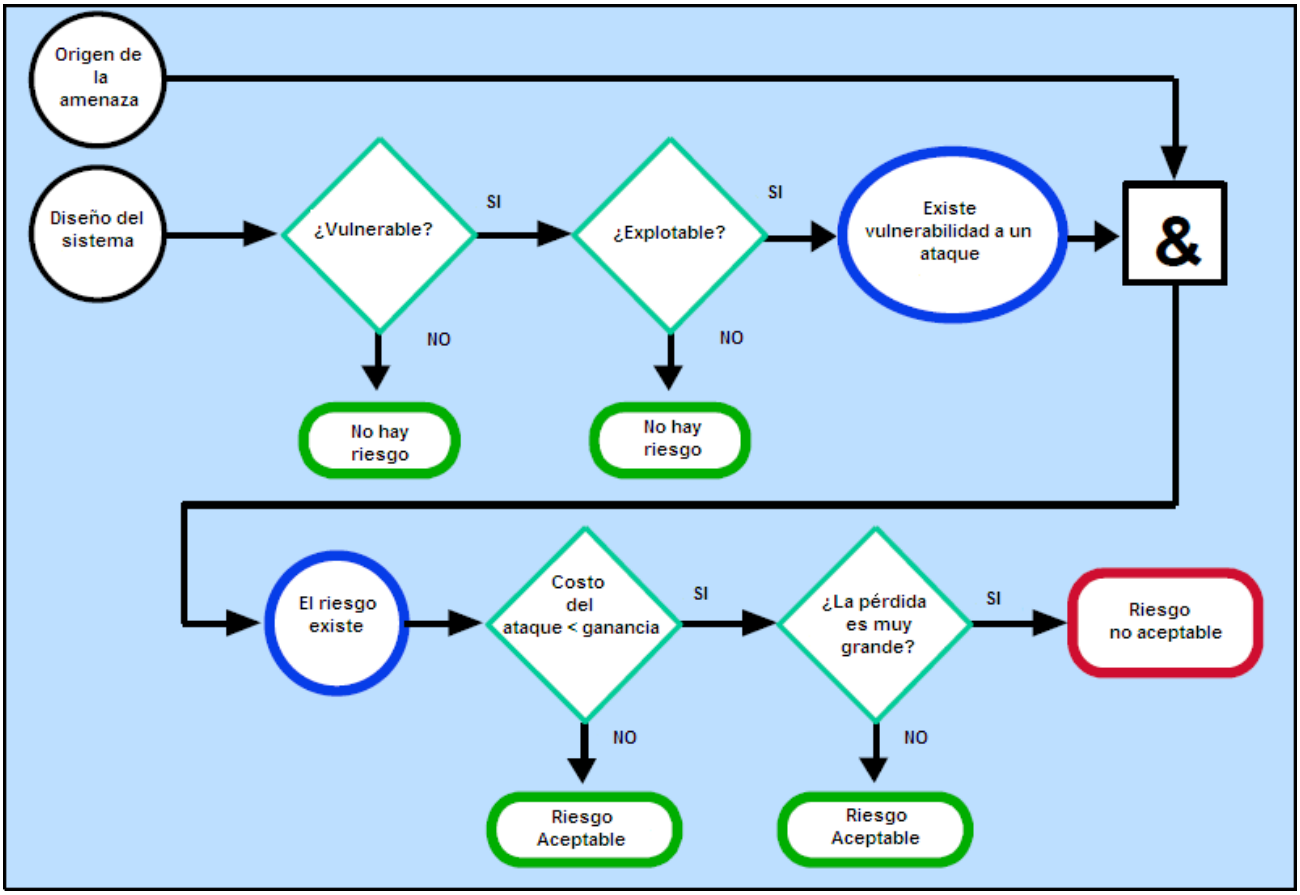


Figura 5.6 Diagrama para la toma de decisiones sobre los riesgos

La interpretación del diagrama de la Figura 5.6 es la siguiente:

Cuando una vulnerabilidad existe, se deben de implementar técnicas para reducir la probabilidad de que una vulnerabilidad sea explotada.

Cuando una vulnerabilidad puede ser ejecutada, se deben aplicar protecciones, diseño de arquitecturas y controles administrativos para minimizar el riesgo de que ocurra un evento desfavorable.

Cuando el costo para el atacante es menor que lo que puede ganar, se deben aplicar protecciones para disminuir la motivación del atacante incrementando el costo del ataque.

Cuando la pérdida es muy grande, se deben aplicar principios de diseño, diseños de arquitectura y protecciones técnicas y no técnicas para limitar el ataque reduciendo el potencial de la pérdida.

Cuando se toma la decisión de implementar acciones para controlar los riesgos, se siguen los siguientes pasos:

Paso 1. Consiste en priorizar las acciones, basándose en los niveles de riesgo presentados en el reporte del Análisis de Riesgos. A la salida de este paso se obtendrá un rango de

acciones clasificados de mayor a menor.

Paso 2. Consiste en evaluar las opciones de control recomendadas. Es posible que los controles recomendados en el Análisis de Riesgos no sean los más apropiados para la organización. Como salida de este paso se obtendrá una lista de los controles más factibles para la empresa

Paso 3. Consiste en realizar un análisis costo–beneficio. Este paso es importante ya que es necesario saber si vale la pena invertir en un control que mitigue un riesgo, si el costo del control es mayor al costo del riesgo la empresa no querrá gastar en el control. Un análisis de costo-beneficio conlleva lo siguiente:

- Determinar el impacto de implementar los nuevos controles.
- Determinar el impacto de no implementar los nuevos controles.
- Estimar los costos de implementación. Estos pueden incluir:
  - Precios de Hardware y Software.
  - Costo de implementar políticas y procedimientos adicionales.
  - Costos de entrenamiento.
  - Costos de mantenimiento.

- Análisis de costo–beneficio de la implementación sobre el sistema y los datos críticos para determinar la importancia para la organización de implementar los nuevos controles dados su costo y su impacto relativo.

Así como existe un precio por implementar los controles, existe un precio por no implementar los controles. Si se decide no implementar un control, será necesario evaluar si la materialización de un riesgo no afecta a la misión de la empresa.

La salida de este paso será el análisis costo–beneficio describiendo los costos y beneficios de implementar y de no implementar los controles.

Paso 4. Consiste en seleccionar los controles. Con base en el análisis costo–beneficio, la administración determinará los controles que reducen los riesgos que afectan a la misión de la empresa. La salida de este paso serán los controles seleccionados.

Paso 5. Consiste en asignar responsabilidades, para esto se seleccionarán personas ya sea internas o externas que tengan el perfil adecuado para implementar el control seleccionado, a estas personas se les asignara la responsabilidad de implementar el control. La salida de este paso consiste en una lista de personas responsables.

Paso 6. Consiste en desarrollar un plan de implementación de los controles. El plan como mínimo deberá de incluir lo siguiente:

- Una lista de amenazas con sus respectivos niveles de riesgo.
- Los controles recomendados.
- Una priorización de acciones.
- Los controles seleccionados.
- Los recursos requeridos para implementar los controles.

- La fecha de inicio para la implementación.
- La fecha prevista en la que se espera haber terminado de implementar los controles.
- Requerimientos de mantenimiento.

A la salida de este paso se tendrá el plan de implementación de controles.

El Paso 7 consiste en implementar los controles seleccionados. Dependiendo de cada situación, los controles pueden disminuir el riesgo pero no eliminarlo completamente, cuando no se elimina existe lo que se llama riesgo residual. La salida de este paso consiste en el riesgo residual.

La implementación de los controles puede mitigar el riesgo de las siguientes maneras:

- Eliminando algunas de las vulnerabilidades del sistema.
- Agregando un control para reducir la capacidad o la motivación que origina una amenaza.
- Reduciendo la magnitud de un impacto adverso.

A pesar de la implementación de controles, realmente no es posible reducir el riesgo a cero, el riesgo resultante después de la implementación de controles se conoce como riesgo residual y éste es asumido por la empresa.

5.4 FRAAP

Facilitated Risk Analysis and Assesment Process (FRAAP) es una metodología cualitativa de Análisis de Riesgos que se basa en otras metodologías del tipo cualitativo, pero que está destinada a ser más rápida y simple en su realización [4]. FRAAP a diferencia de las otras metodologías, para identificar los Riesgos de la organización se basa en los procesos de negocio de la empresa y no tanto en aspectos relacionados con las tecnologías de información. La característica principal de esta metodología es una sesión llamada Sesión FRAAP, que es donde se identifican las vulnerabilidades de la empresa, pero para poder realizarla se siguen las siguientes fases de esta metodología:

PRE-FRAAP. Esta fase de la metodología consiste en realizar los preparativos para poder realizar de manera adecuada la Sesión FRAAP.

Durante este paso de la metodología se organizará una reunión con el dueño de la empresa o un representante de él, esta reunión tiene por objetivo lo siguiente:

- Preseleccionar los objetivos. Durante la sesión FRAAP no se podrán revisar todos los detalles acerca de los procesos de negocio y aplicaciones que se tienen, es importante seleccionar cuales son los que tienen mayor peso para la empresa, para ello el dueño de la empresa deberá indicar cuál es la información más importante y cuáles son las aplicaciones que trabajan con dicha información, de esta forma se podrá acotar el alcance de la sesión.

- Realizar un modelo visual. Este modelo es un diagrama de no más de una hoja, el cual describirá los procesos que se revisarán en la sesión y durante dicha sesión servirá para delimitarla, es decir, indicara cuándo inicia y en qué momento termina.

- Establecer el equipo FRAAP. Este equipo es el que se reunirá en la sesión FRAAP, constará de 15 a 30 personas y estará formado por representantes de diferentes áreas del negocio y del área de Tecnologías de Información. Los representantes sugeridos son:

    - Dueño del negocio.
    - Usuarios del sistema.
    - Analistas del sistema.
    - Programadores.
    - Administradores de Bases de Datos.
    - Encargados de redes y comunicaciones.
    - Representantes del área de administración y finanzas.

    A parte de estos representantes, para poder llevar a cabo la sesión adecuadamente, son necesarios los siguientes personajes:

    - Facilitador. Una persona capacitada en la metodología FRAAP.
    - Experto en la materia. Es una persona de la organización donde se está realizando el Análisis de Riesgos, la cual posee conocimiento de los procesos de negocio de la empresa.
    - Anotador. Esta persona se encarga de documentar los sucesos de la sesión.

- Preparar el escenario para la sesión FRAAP. Este aspecto correrá a cargo del dueño o representante de la empresa, ya que consiste en conseguir el lugar donde se hará la sesión, así como el día, la hora y los materiales necesarios. Para lograr esto, el facilitador le asistirá para completar el escenario de la forma más adecuada posible.

- Por último se darán a conocer los conceptos básicos que son necesarios para poder realizar el Análisis de Riesgos. Estos conceptos se mencionaron al final del Capítulo 1.

Sesión FRAAP. En esta fase de la metodología es donde se identifican las diferentes amenazas que existen para la empresa, se determina su nivel de riesgos y los posibles controles que existen para las amenazas. En esta sesión será llevada a cabo con el equipo FRAAP, donde el Facilitador deberá ser quien dirija a las personas que participen para poder identificar las amenazas, establecer el nivel de riesgo determinado por su probabilidad de ocurrencia e impacto y sus respectivos controles y salvaguardas.

Debido a que el Análisis de Riesgos cualitativo es de naturaleza subjetiva, el Facilitador deberá dirigir al equipo en diferentes áreas de la empresa con el fin de identificar el mayor número de amenazas posibles.

Durante la sesión el Facilitador deberá seguir las siguientes reglas:

- Observar respuestas no verbales.
- Nunca leer, escuchar e involucrar al equipo en la sesión.
- Nunca olvidar el objetivo de la sesión.
- Permanecer neutral o al menos simular serlo.

Es importante saber escoger a la persona que llevará a cabo el rol de Facilitador, pues su labor, aparte de realizar todas las funciones mencionadas, es lograr mantener la atención los miembros del equipo FRAAP, evitar discusiones entre ellos y lograr motivarlos para que participen y cada uno de los miembros del equipo de sus puntos de vista.

Una vez identificados las diferentes amenazas para la empresa, se seleccionarán aquellas que afecten en mayor medida a la empresa, y de éstas amenazas, se deberá identificar qué controles son los que tienen actualmente, el nivel de riesgo que representa para la empresa, los controles adecuados para disminuir el riesgo y las personas responsables para implementar los controles para dichas amenazas.

Una vez completada la sesión FRAAP y se hayan identificado las amenazas, el nivel de riesgo que representan las amenazas para la empresa y los controles de las amenazas, se podrá pasar a la siguiente etapa de la metodología.

POST – FRAAP. Esta fase de la metodología tiene como finalidad generar un reporte que contendrá los riesgos evaluados así como la forma de administrarlos a fin de poderlos reducir a un nivel aceptable.

Durante esta fase tanto el Facilitador como el dueño de la empresa deberán trabajar en un plan de acción para poder llevar a cabo la mitigación de los riesgos, para ello se usarán los resultados de la sesión FRAAP, los cuales son:

- Amenazas identificadas.
- Niveles de riesgo establecidos.
- Posibles controles sugeridos.
- Controles existentes identificados.
- Controles seleccionados para algunas amenazas específicas.

Al final del Análisis se deberá entregar un Resumen Administrativo, el cual deberá incluir:

- Metodología utilizada.
- Principales amenazas junto con sus controles correspondientes.
- Recomendaciones de los expertos.
- Anexos.

5.5 Análisis Comparativo entre las diferentes Metodologías.

En este capítulo se han visto diferentes metodologías para la realización del Análisis de Riesgos. Estas metodologías si bien no son todas las qué existen, sí son las más completas.

Algunas metodologías realizan el análisis con un enfoque cuantitativo, otras lo realizan con un enfoque cualitativo, otras lo pueden realizar de ambas maneras, pero solo una a la vez.

Se ha mencionado que las diferentes metodologías realizan el Análisis de Riesgos compartiendo algunas características, tales como la identificación de activos, identificación de vulnerabilidades, identificación de amenazas y determinación de riesgos. Aunque todas las metodologías comparten la misma finalidad, también poseen características que las hacen distintas. Conocer las diferentes ventajas y desventajas de las metodologías es lo que permitirá escoger la metodología adecuada en el momento de realizar el Análisis en las diferentes empresas.

La Tabla 5.1 muestra las características, ventajas y desventajas de las metodologías que se han explicado a lo largo de este capítulo.

Metodología	Enfoque	Número de Pasos	Característica Principal	Ventajas	Desventajas
OCTAVE	No define, pero sus características son las de un análisis cualitativo	Tres fases que contienen en total 8 procesos	Muy detallada en sus diferentes fases y es la más completa	Contiene ejemplos detallados en sus diferentes fases contemplando detalles que otras metodologías no cubren.	Puede resultar muy complejo seguir esta metodología al pie de la letra. Para realizar el Análisis con esta metodología puede tomar mucho tiempo, dependiende del tamaño de la empresa.
MAGERIT	Principalmente cuantitativo aunque también puede ser cualitativo, no obstante la metodología no lo recomienda	Cinco pasos	Contiene un catálogo de elementos que facilita la identificación de activos, amenazas y salvaguardas	Sus resultados son objetivos y arrojan un valor monetario sobre las diferentes amenazas. Un directivo entiende mejor si se le dice cuánto cuesta un riesgo que si se le dice que el riesgo es alto, medio o bajo.	Es difícil realizar el Análisis de riesgos con esta metodología pues es susceptible a errores en la cuantificación del riesgo. Requiere también de datos con los cuales no necesariamente cuentan las empresas, lo que retrazará el Análisis
NIST 800-30	Cualitativo	Nueve pasos mas siete pasos adicionales para la mitigación de riesgos	Describe los diferentes pasos de forma muy general, sin embargo contempla la mitigación de riesgos	Es una metodología creada con la finalidad de convertirse en un estándar. A pesar de ser una metodología bastante simple, contiene un proceso para poder decidir que se realizará con los riesgos encontrados.	Menciona diferentes técnicas que pueden ser usadas en el análisis pero no los describe. Describe los pasos del Análisis de una forma muy general, haciendo que sea necesario complementar el Análisis.
FRAP	Cualitativo	Tres fases	En una sesión con diferentes elementos de la empresa puede obtener los principales riesgos de la empresa	Es la metodología que realiza el Análisis de Riesgos en el menor tiempo. Al involucrar a la gente que trabaja en las empresas obtiene perspectivas importantes que una persona externa dificilmente puede conocer.	Es difícil y tardado conseguir que diferentes elementos de la empresa se puedan juntar para realizar la sesión. Dificilmente cualquier persona podrá dirigir la sesión donde se identifican las amenazas que tiene la empresa.

Tabla 5.1 Comparación entre las diferentes Metodologías.

Como se puede observar en la Tabla 5.1, de todas las metodologías **OCTAVE** es la más detallada, contempla diferentes aspectos previos al Análisis de Riesgos y ejemplifica de forma clara como evaluar los activos y obtener las amenazas e impactos. Es una metodología robusta y habrá detalles que no se apliquen a algunas empresas en específico. Si se decide utilizar alguna otra metodología, es útil leer los volúmenes que contienen a la metodología OCTAVE, pues en ellos se encuentra información que puede ser usada en el proceso de análisis de las otras metodologías. OCTAVE no especifica si se basa en el enfoque cuantitativo o cualitativo, no obstante en los volúmenes que contienen a la metodología no se explica cómo realizar el análisis de forma cuantitativa, más bien por sus

características es más válido pensar que es una metodología basada en el enfoque cualitativo.

La metodología propuesta por el NIST en su publicación **800-30** puede ser aplicable para diferentes tipos de empresas, no obstante su principal objetivo son los organismos de gobierno (principalmente de los Estados Unidos), es decir, en esta metodología se presupone que las instituciones de gobierno ya comprenden la importancia del Análisis de Riesgos, e incluso que es algo mandatorio para dichas instituciones, algo que no ocurre en otro tipo de empresas. Los pasos de esta metodología son simples, sin embargo llevarlos a la práctica supondrá un esfuerzo extra ya que esta metodología indica lo que se tiene que hacer, pero no cómo hacerlo.

La metodología **MAGERIT** aunque puede basarse en un enfoque cualitativo, principalmente se basa en un enfoque cuantitativo, el cual es más laborioso y tardado, incluso la misma metodología señala que es difícil llevarlo a cabo, no obstante, si previamente se llevó un registro de todos los incidentes de seguridad que hayan ocurrido en los años previos a la realización del análisis, dicha información permitirá avanzar más rápido en el análisis y obtener resultados más concretos que los que se pueden obtener con un análisis basado en un enfoque cualitativo, no obstante la realidad es que la mayoría de las empresas no tienen este tipo de información, principalmente debido a la falta de documentación sobre los incidentes de seguridad, por lo cual si se intenta realizar el Análisis de Riesgos sin esa información, el proceso del análisis aumentará en tiempo.

Uno de los objetivos de la metodología **FRAAP** es lograr realizar el Análisis de Riesgos en el menor tiempo posible. Esta metodología señala que un Análisis de Riesgos no debe tomar meses en realizarla y pretende realizar el Análisis de Riesgos idealmente en una semana, pero la realidad es que es una semana lo que se tardaría el Análisis una vez que se hayan realizado ciertas actividades previas, las cuales incluyen el obtener el apoyo de la gerencia (que nadie dice como obtener), también es necesario poder reunir a la gente que participara en la sesión en la cual se identificarán las amenazas y vulnerabilidades de los activos. Poder conseguir que diferentes perfiles de la empresa puedan apartarse de sus actividades para poder realizar la sesión tampoco viene especificado dentro de la metodología y poder reunir a los integrantes para la sesión tomará más tiempo. Sin embargo, una vez superados esos problemas, esta metodología permitirá realizar el Análisis de Riesgos más rápido incluso que otras metodologías que se basen en un enfoque cualitativo.

Algo en lo que coinciden la mayoría de las metodologías es que es importante conseguir el apoyo de la gerencia, dicho apoyo es fundamental para poder realizar el análisis, ya que si no se cuenta con dicho apoyo, los empleados de la empresa por sí mismos no le darán la importancia a este análisis y no se obtendrá su cooperación para poder identificar las diferentes amenazas y riesgos para los activos de la empresa. Es por ello que se necesita el apoyo de la gerencia, los empleados al ver que el dueño de la empresa o la gerencia dan su apoyo al análisis, cooperarán en el análisis; sin embargo, todas las metodologías a pesar de resaltar la importancia de este apoyo, ninguna dice cómo conseguirlo.

5.6 Resultados del Análisis Comparativo

Independientemente de la metodología que se escoja para realizar el Análisis de Riesgos, es

útil revisar las demás metodologías, ya que ofrecen puntos de vista diferentes que pueden enriquecer el proceso del Análisis.

La metodología propuesta por el NIST puede usarse bajo el enfoque cuantitativo o cualitativo, no obstante no indica cómo realizar el análisis cuantitativo. Esta metodología es la más simple de todas y a diferencia de las otras metodologías que indican que es lo que hay que hacer y cómo hacerlo, la metodología 800-30 sólo da las pautas sobre cómo hacerlo, es decir, realizar el análisis por medio de esta metodología requerirá de un trabajo extra por parte de quienes deseen utilizar esta metodología, por lo cual si es el primer Análisis de Riesgos que se realiza en una empresa será mejor optar por otra metodología.

De las metodologías que realizan el Análisis de Riesgos desde el enfoque cuantitativo, MAGERIT es una muy buena opción, ya que esta metodología fue hecha específicamente para realizar el análisis cuantitativo y explica cómo realizarlo. Tiene una ventaja extra y es que esta metodología fue desarrollada directamente en el idioma español, lo cual podrá evitar problemas de interpretación en la traducción; sin embargo, como se ha mencionado anteriormente, realizar un Análisis de Riesgos Cuantitativo no es una labor sencilla y puede llegar a tomar mucho tiempo para poder reunir la información necesaria para su realización, y si un proyecto de cualquier naturaleza se extiende mucho en tiempos, resultará poco atractivo para los fines de la empresa.

De estas 4 metodologías, OCTAVE y FRAAP al ser de naturaleza cualitativa permiten realizar el Análisis de Riesgos de menara más ágil. A pesar de ambas metodologías utilizan el mismo enfoque, presentan diferencias significativas entre ellas. La ventaja que tiene FRAAP sobre OCTAVE radica en el hecho de que si se realiza eficientemente, FRAAP puede llegar a realizar el análisis en menos tiempo que con otras metodologías, ya sean de enfoque cuantitativo o cualitativo, y a pesar de que el Análisis de Riesgos es realizado en menor tiempo, ello no significa que los resultados carezcan de importancia puesto que se basan principalmente en las necesidades de la empresa.

A continuación se muestran los resultados que se obtienen con las metodologías OCTAVE y FRAAP.

5.7 Resultados obtenidos con las metodologías OCTAVE y FRAAP

Como ya se ha mencionado, OCTAVE y FRAAP son dos buenas opciones para realizar el Análisis de Riesgos, a continuación se muestra un ejemplo de los resultados de utilizar ambas metodologías.

5.7.1 Resultados obtenidos con la metodología OCTAVE

El Análisis de Riesgos realizado a través de la metodología OCTAVE después de seguir los pasos que incluye en su metodología, llega a los resultados que se muestran en la Figura 5.7, los cuales muestran los riesgos que se encontraron después de haber realizado el Análisis a una institución de educación universitaria. En este ejemplo, los resultados presentan al activo que se analizó, en este caso es el servidor de la base de datos, a la cual se puede acceder por medio de la red de la institución, el actor que puede acceder a la red en este caso puede ser alguien interno o externo a la institución, en cada caso el actor podrá

acceder de forma intencionada o accidental, lo cual genera diferentes consecuencias, como el hecho de que la información sea revelada, modificada o que se interrumpa el servicio usado para consultarla, una vez identificadas las salidas o consecuencias, se procede a estimar el nivel de impacto que representa para la institución.

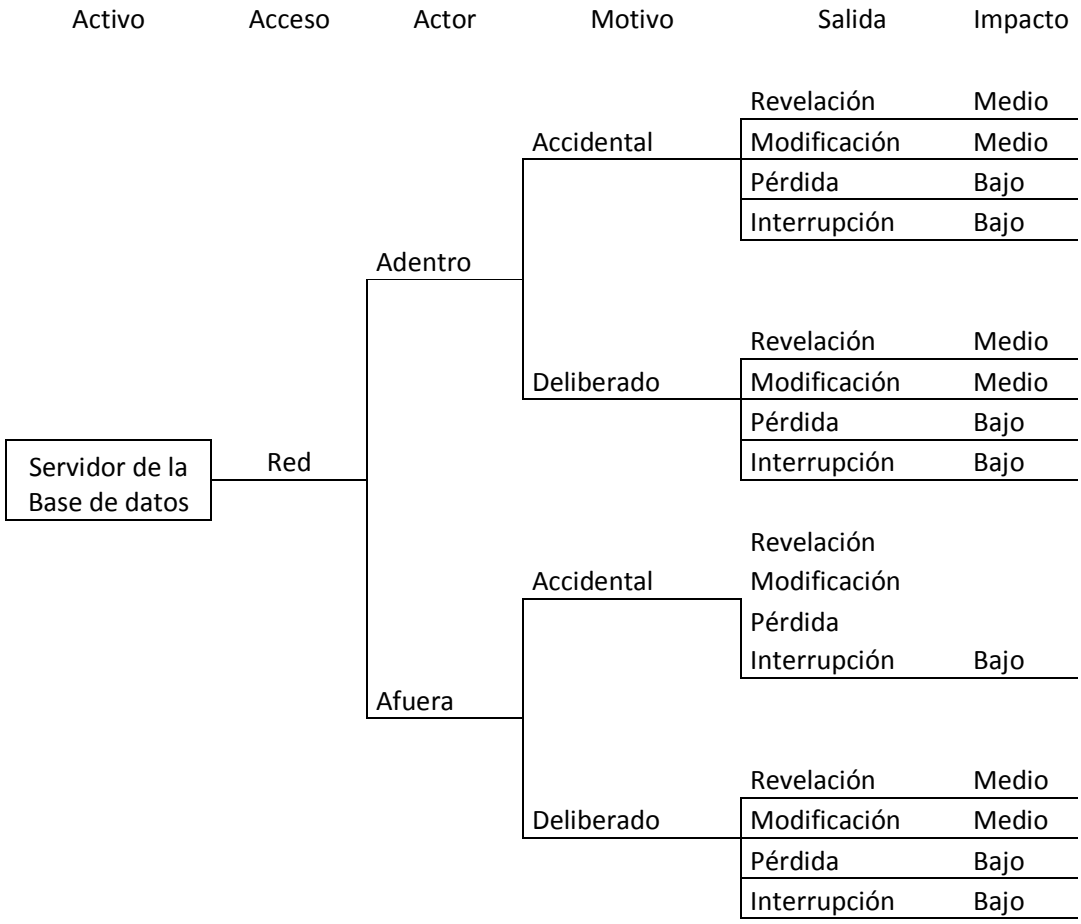


Figura 5.7 Resultados obtenidos con la metodología OCTAVE.

Por medio de la metodología OCTAVE los riesgos son identificados como se vio en la Figura 5.7, los resultados anteriormente expuestos nos muestran las vulnerabilidades que tiene una empresa así como las consecuencias de que éstas se materialicen y su nivel de riesgo. Estas vulnerabilidades deberían de ser corregidas por medio de la implementación de controles, no obstante es necesario decidir cuáles son las vulnerabilidades que se van a controlar, pues como se ha mencionado anteriormente, no es posible corregir todas las vulnerabilidades de una empresa. La decisión acerca de qué vulnerabilidades han de ser corregidas será decisión de los dueños de la empresa, pues son ellos quienes mejor conocen los intereses que pretenden obtener, para ello los resultados arrojados por la metodología OCTAVE le dará un panorama de las vulnerabilidades de su empresa, sin embargo solo indican que grado de riesgo representan las vulnerabilidades y no necesariamente las que más afectan a la empresa.

5.7.2 Resultados obtenidos con la metodología FRAAP

Los resultados a los que se llega después de haber realizado el Análisis de Riesgos a una institución bancaria a través de la metodología FRAAP son los que se muestran en la Figura 5.8, en la cual como se puede apreciar, los resultados están clasificados en cuanto a su nivel de vulnerabilidad e importancia relativa. En este caso lo que se representa en la figura son las acciones que se deben de llevar a cabo para proteger a los activos de la empresa, cuando más alta sea su importancia relativa y su nivel de vulnerabilidad, la acción indicada deberá tener una prioridad alta para los intereses de la empresa y como se puede apreciar en la figura, a la institución bancaria lo que más le preocupa son los Respaldos, Control de Acceso y la Planeación de la Continuidad del Negocio.

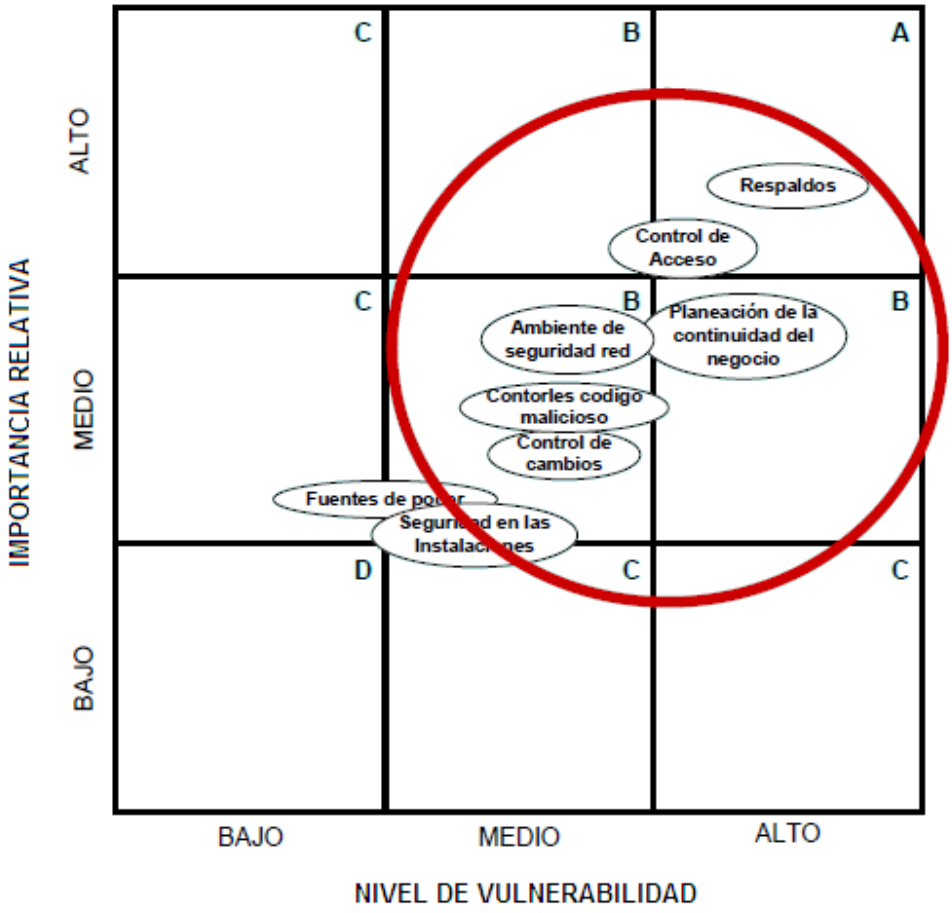


Figura 5.8 Resultados obtenidos con la metodología FRAAP.

La Figura 5.8 muestra los resultados obtenidos a través de la metodología FRAAP. Los resultados arrojados por FRAAP, como se puede ver, no solo muestran los riesgos identificados a través de la metodología y el nivel de las vulnerabilidades que tiene la empresa en cuanto a su importancia relativa sino que también indica las amenazas que más le preocupan a la empresa. En esta metodología, al haber tenido la participación de diferentes perfiles de la empresa, sus resultados reflejarán las preocupaciones de las diferentes áreas de la empresa. En otras palabras, esta metodología a la hora de entregar

sus resultados ya muestra cuáles son las amenazas que más afectan a la organización. Desde luego los dueños del negocio pueden escoger mitigar los riesgos que ellos consideren más adecuados, no obstante los resultados que se muestran en la Figura 5.8 facilitan esa decisión, lo cual es una ventaja extra a parte de la reducción del tiempo en el Análisis.

FRAAP es recomendable si la empresa donde se va a realizar un Análisis de Riesgos nunca antes había realizado dicho Análisis, pues al no requerir datos previos y obtener la información directamente de las personas involucradas del negocio, realiza el Análisis de forma más simple y rápida, obteniendo resultados que estarán alineados a las necesidades de la empresa. Aunque OCTAVE también es una buena metodología, por mucho que se pretenda realizar el análisis de forma más ágil, no se pueden obtener los resultados tan rápido como con la metodología FRAAP y para cualquier empresa es importante minimizar los tiempos de cada uno de sus procesos.

En el momento de realizar un Análisis de Riesgos seguir una metodología es útil, no obstante realizar el Análisis únicamente de acuerdo a lo que esta descrito en las metodologías no es suficiente, pues en éstas se omiten muchas cosas, como por ejemplo cómo conseguir el apoyo de la gerencia o de los dueños de la empresa, cómo reunir la información de los incidentes ocurridos en la empresa para sacar los datos necesarios para realizar un análisis cuantitativo o cómo poder reunir a diferentes miembros de una misma empresa para poder realizar una sesión donde se identificarán las amenazas de la empresa.

Para poder realizar el Análisis de Riesgos será bueno seguir los pasos que se encuentran en una metodología sin embargo eso no bastará, también es necesario utilizar el sentido común y la experiencia para poder realizar todo lo que no está descrito en las metodologías.

A lo largo de los capítulos anteriores se ha hablado de lo que es la Seguridad de la Información, se describió el ciclo de vida de la Seguridad Informática, se describieron diferentes estándares de seguridad y se vio la importancia del Análisis de Riesgos junto con las metodologías que se pueden seguir para realizarlo, no obstante, como se vio en la comparación de las diferentes metodologías, hay detalles importantes que no están claramente descritos y que sin embargo al momento de pasar a la práctica pueden significar un retraso en los tiempos estimados para la realización del Análisis, es por ello que es posible llegar a las conclusiones que se presentan en el siguiente capítulo.

Referencias Capítulo 5

1 *CERT ® Coordination Center* **“OCTAVE Method Implementation Guide”.** Versión 2. Metodología publicada por OCTAVE® Carnegie Mellon University en Estados Unidos en el año 2001. Disponible en: http://www.cert.org/octave/octavemethod.html

2 *Francisco López Crespo, Miguel Angel Amutio Gómez, Javier Candau, José Antonio Mañas.* **“Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información”.** Versión 2. Metodología publicada por el MINISTERIO DE ADMINISTRACIONES PÚBLICAS en España en el año 2006. Disponible en: http://www.csae.map.es/csi/pdf/magerit_v2/metodo_v11_final.pdf

3 *Gary Stoneburner, Alice Goguen, Alexis Feringa* **“Risk Management Guide for Information Technology Systems”.** National Institute of Standards and Technology Publicación Especial 800-30. Metodología publicada por el Departamento de Comercio de los Estados Unidos en Estados Unidos en el año 2002.

4 *Thomas R. Peltier* **“Information Security Risk Analysis”.** Ed. Taylor & Francis Group. Segunda Edición. Publicado en Estados Unidos el año 2005.

Capítulo

6

Conclusiones y Recomendaciones.

6 Resultados y Conclusiones.

Resultados

En este trabajo se han revisado diferentes estándares de seguridad, algunos de ellos poseen ciertas similitudes, otros hablan de situaciones más especificas, no obstante es importante conocerlos para poder así obtener una mejor visión a cerca de las mejoras que se le pueden aplicar a una empresa.

De los estándares mostrados en el Capítulo 3, el ISO 17799 resalta que es importante realizar una Evaluación y Tratamiento de riesgos, lo cual viene siendo la Administración de Riesgos. Dentro de la Administración de Riesgos, el primer paso es realizar un Análisis de Riesgos, el cual más adelante servirá como base para poder realizar la correcta Administración de los Riesgos.

El ser el Análisis de Riesgos el primer pasó dentro de la Administración de Riesgos, hace que sea importante llevarlo a cabo de forma correcta, ya que las decisiones que se tomen después dependerán de los resultados obtenidos en el Análisis, y si el Análisis es realizado de forma equivocada significará una pérdida de tiempo, dinero y recursos, algo que es indeseable en cualquier empresa.

Para realizar correctamente un Análisis de Riesgos es recomendable utilizar una Metodología. Las metodologías presentadas en este trabajo han sido desarrolladas por diferentes instituciones, cuya finalidad es que empresas de diferentes naturalezas puedan realizar de manera eficiente el Análisis. Cada metodología tiene la misma finalidad, no obstante difieren en su forma de realizar el Análisis de Riesgos. Cuando se hizo la comparación entre las metodologías se indicaron las diferencias que existen entre ellas así como sus ventajas y desventajas.

De las metodologías revisadas en este trabajo, como ya se mencionó, FRAAP posee una ventaja sobre las demás metodologías, la cual no solo radica en el hecho de realizar el Análisis más rápidamente que otras metodologías sino que también toma en cuenta las necesidades del negocio.

Sin embargo, a pesar de que las metodologías marcan el camino para realizar el Análisis de Riesgos, ninguna de ellas puede realizarse sólo basándose en la metodología, es necesario utilizar el sentido común y la experiencia. Existen herramientas que pueden encontrar vulnerabilidades o riesgos de las empresas, no obstante por sí solas no pueden tomar decisiones acerca de cuál es la mejor forma de solucionar los problemas de seguridad de las empresas o saber qué es lo más importante para una empresa, al menos hasta ahora sigue siendo indispensable la participación humana en este tipo de procesos.

Después de haber realizado el Análisis de Riesgos, es importante enfocarse a cubrir los requerimientos de seguridad hallados en el Análisis y no tratar de cubrir mas allá de lo señalado por el Análisis, pues como ya se ha mencionado, la seguridad no es algo que sea barato de implementar y si se empiezan a cubrir detalles que no son necesarios no solo aumentarán los costos, sino que se terminará afectando a la operación de la empresa.

En base al proceso de haber realizado este trabajo es que se pudo llegar a las conclusiones siguientes:

Conclusiones

Como se ha mencionado anteriormente, la tecnología que usamos día con día fue diseñada para ser fácil de usar, y el problema no acaba ahí, actualmente la tecnología sigue creciendo a un ritmo acelerado donde se busca cubrir diferentes necesidades de los usuarios con la finalidad de participar en un mercado cada vez mas demandante, y es debido a ello que existen diferentes incidentes de seguridad donde se explotan diferentes vulnerabilidades de las cuales en muchas ocasiones no se tenía conciencia de su conocimiento hasta que llegó un individuo que de alguna forma encontró la vulnerabilidad y la aprovechó en su beneficio.

La Seguridad Informática tiene la finalidad de poder lograr que las personas y empresas puedan operar sus equipos y realizar sus actividades de manera segura, evitando así no sólo que atacantes afecten a la integridad de la información, sino que también debe evitar los incidentes de seguridad causados de manera accidental.

En el caso de las empresas, éstas buscan poder operar de manera continua con la finalidad de incrementar sus ganancias; sin embargo, si bien es cierto que la Seguridad Informática le da continuidad al negocio, también es cierto que la seguridad corre en sentido opuesto a la operación de la empresa, es por ello que surge la pregunta: ¿Cuánta seguridad es suficiente para una empresa?, ¿poca o mucha?

Mientras más seguridad se le quiera dar a una empresa, más impacto se tendrá sobre la operación de la misma. En el área de seguridad cualquier medida que se implemente tendrá un precio. Por ejemplo, algo sencillo como implementar una política que obligue a los usuarios a usar un password de al menos 8 caracteres con mayúsculas y minúsculas tendrá un impacto en la flexibilidad para los usuarios legítimos de los equipos.

No obstante, implementar seguridad en una empresa pudiera no resultar suficiente si no se toma en consideración que la seguridad no es un proceso en el cual se analiza a la empresa, se determinan los riesgos que enfrenta, se toman las medidas adecuadas para mitigar los riesgos y la empresa puede continuar operando. Como se vio en el Capítulo 2, la seguridad tiene un ciclo de vida el cual se repite constantemente, es decir, no basta con llegar y asegurar a una empresa, hay que mantener la seguridad en un proceso constante, esto debido a que sabemos que las tecnologías, las personas y otros factores internos y externos a la empresa se mantienen cambiando constantemente.

Si una empresa quiere implementar seguridad y comienza a hacerlo sin un orden, puede llegar a desperdiciar sus recursos y posiblemente no lo consiga, para evitar que eso suceda es importante realizar un Análisis de Riesgos. Los conceptos de Análisis de Riesgos y Administración de Riesgos son conceptos relativamente nuevos y aún se requiere tomar conciencia de su importancia.

Es importante realizar una adecuada Administración de Riesgos pues aunque los riesgos se transfieran a una compañía externa, ésta jamás cubrirá la pérdida de mercado, clientes,

imagen, personal capacitado y muchos otros aspectos que resultan intangibles, los cuales si bien no tienen un valor monetario, si afectan de alguna forma a la empresa.

Como se ha visto, es importante conocer los diferentes riesgos que tiene la empresa en el momento de su operación, sin embargo realizar una Administración de Riesgos tampoco es algo sencillo de hacer, no se puede administrar el riesgo si no se conoce que amenazas pueden llegar a afectar a la misión de la empresa, es por ello que cobra importancia el Análisis de Riesgos.

Para realizar el Análisis de Riesgos existen dos enfoques: el enfoque cuantitativo y el enfoque cualitativo, cada uno presenta sus ventajas y desventajas. Un análisis cuantitativo es mas objetivo y arroja información que puede ser estudiada más a detalle, un análisis cualitativo no arroja tanta información, pero permite realizar el análisis más rápido y con menos requerimientos que el cuantitativo.

Aunque sería ideal realizar un análisis cuantitativo, la realidad es que las empresas por diferentes razones no documentan la información de los incidentes de seguridad por los que han pasado, esto hace que no se tenga información suficiente para realizar adecuadamente un análisis cuantitativo, y realizar un mal Análisis de Riesgos puede ser más contraproducente que no hacer nada, ya que lo peor que se puede hacer en cuanto a la seguridad de la información no es el hecho de no hacer nada, lo peor es tener un falso sentido de la seguridad, es decir, creer que funcionará un control para mitigar un riesgo cuando en realidad el control pudiera no funcionar, o bien el riesgo que se está mitigando no afecta a la empresa de forma tan significativa como para que se justifique implementar medidas al respecto.

Debido a la falta de documentación sobre los incidentes de seguridad que han ocurrido es más factible realizar un Análisis de Riesgos con enfoque Cualitativo utilizando la metodología FRAAP, ya que no sólo permitirá realizarlo más rápidamente, sino que se puede trabajar sin el conocimiento de la documentación de los incidentes de seguridad ocurridos antes de la realización del análisis y pese a ello arroja resultados que están basados en las necesidades de negocio de la empresa.

Una vez realizado el Análisis de Riesgos e implementados los controles necesarios para mitigar los riesgos encontrados, es importante empezar a recolectar información sobre los diferentes incidentes de seguridad que ocurren en la empresa, documentar el funcionamiento de los controles y evaluar periódicamente la seguridad, a fin de poder obtener información que le permita a la empresa generar estadísticas con la finalidad de que en un futuro se pueda tener la información necesaria para realizar un Análisis de Riesgos Cuantitativo, aunque si la empresa evalúa y encuentra que le satisfacen los resultados obtenidos con una metodología cualitativa como FRAAP se puede seguir trabajando con esa metodología, pues los resultados obtenidos son válidos y se tiene la ventaja de que es un análisis sencillo y rápido.

Sin embargo realizar el Análisis de Riesgos no lo es todo, también importante conocer los diferentes estándares y buenas prácticas de seguridad que existen, no obstante, mas importante aún es poder identificar cuáles son las medidas que mejor funcionan para la empresa en la que se está implementando la seguridad, ya que los problemas de seguridad que tiene una empresa en particular, no son los problemas a los que se enfrentan las demás empresas. En este aspecto, más importante que obtener una certificación en un estándar, es

lograr distinguir las buenas prácticas que le funcionan a la empresa donde se implementará la seguridad, es por ello que es fundamental conocer a la empresa ya que conociendo a la empresa será como se logrará distinguir las medidas de seguridad que funcionarán. También es igual de importante no sólo identificar las medidas que funcionan sino que hay que llevarlas a cabo de forma continua y buscar nuevas amenazas y medidas de seguridad, ya que la seguridad como cualquier sistema se mantiene en un proceso que cambia constante, donde si el día de hoy se corrigió una falla con algún mecanismo, es probable que el día de mañana ese mecanismo será obsoleto.

Referencias

Libros

Eric A Fish, Gregory B. White **"Secure Computers and Networks: Analysis, Design, and Implementation".** Ed. CRC Press. Primera Edición. Publicado en Estados Unidos en el año 1999.

Bill McCarty **"El Libro oficial de Red Hat Linux firewalls".** Ed. Anaya. Primera Edición. Publicado en España en el año 2003.

James Michael Stewart Mike Chapple **"CISSP: Certified Information Systems Security Professional Study Guide".** Ed. Tittel *Mike Chapple.* Tercera Edición. Publicado en Estados Unidos en el año 2005.

Rolf Oppliger **"Contemporary Cryptography".** Ed. Artech House. Primera Edición. Publicado en Estados Unidos en el año 2005.

Bruce Schneier **"Applied Cryptography: Protocols, Algorithms, and Source Code in C".** Ed. John Wiley & Sons, Inc. Segunda Edición. Publicado en Estados Unidos en el año 1996.

Enrique Daltabuit Godás, Leobardo Hernández Audelo, Guillermo Mallén Fullerton, José de Jesús Vázquez Gómez. **"La seguridad de la información".** Ed. Limusa Noriega Editores. Primera Edición. Publicado en México en el año 2007.

Thomas R. Peltier **"Information Security Risk Analysis".** Ed. Auerbach Publications. Segunda Edición. Publicado en Estados Unidos en el año 2005.

Internet

ITSecurity **"Top 10 Most Famous Hackers of All Time".** Página Web disponible en: http://www.itsecurity.com/features/top-10-famous-hackers-042407/ Leído por última vez el 28 de septiembre de 2009.

Universidad de Alicante. **"VIRUS ILOVEYOU".** Página Web disponible en: http://www.ua.es/es/novedades/comunicados/2000/iloveyou.htm Leído por última vez el 28 de septiembre de 2009.

VSantivirus **"Condenado el autor del virus Kournikova".** Página Web disponible en: http://www.vsantivirus.com/29-09-01.htm Leído por última vez el 28 de septiembre de 2009.

Magnus Daum, Stefan Lucks **"Hash Collisions (The Poisoned Message Attack) "The Story of Alice and her Boss"".** Página Web disponible en: http://th.informatik.uni-mannheim.de/People/lucks/HashCollisions/ Leído por última vez el 28 de septiembre.

NIST **"Federal Information Processing Standards Publications".** Página Web disponible en: http://www.itl.nist.gov/fipspubs/by-num.htm Leído por última vez el 28 de septiembre de 2009.

Wikipedia The Free Encyclopedia. **"Security Controls".** Disponible en: http://en.wikipedia.org/wiki/Security_controls Leído por última vez el 28 de septiembre de 2009.

Ernesto Perez **"ROSI (Return on Information Security Investment)".** Página Web disponible en: http://pastorcortes.net/rosi_return_on_information_security_investment_ Leído por última vez el 2 de octubre

de 2009.

Publicaciones

ISO/IEC 17799 **“Information Technology – Code of practice for information security management”.** Primera Edición. Estándar publicado por International Organization for Standardization en Suiza en el año-2000.

ISO 7498-2 **“Information processing systems - Open Systems Interconnection - Basic Reference Model Part 2 Security Architecture”.** Primera Edición. Estándar publicado por International Organization for Standardization en Suiza en el año 1989.

Roberto Gómez Cárdenas **“La esteganografía”.** Revista Bsecure. Editorial Netmedia. Publicada en México en el año 2004.

Leonardo García Rojas **“The information security process under BS7799/ISO17799”.** Paper Publicado en Nebraska Cert Conference realizada en Estados Unidos en el año 2005 Disponible en: ohttp://www.certconf.org/presentations/2005/files/WA1.pdf

Computer Security Division NIST **“INFORMATION SECURITY IN THE SYSTEMS DEVELOPMENT LIFE CYCLE”.** Versión 2. Publicado por el National Institute of Standards and Technology en Estados Unidos en el año 2007. Disponible en: http://csrc.nist.gov/groups/SMA/sdlc/index.html

Lee Wan Wai **“Security Life Cycle”.** White Paper Versión 1. Publicado por SANS Institute en Estados Unidos en el año 2001. Disponible en: http://www.sans.org/reading_room/whitepapers/testing/security_life_cycle_1_diy_assessment_260?show=260.php&cat=testing

ISO/IEC 27001:2005 **“Information Technology – Security techniques – Information Security Management Systems - Requeriments”.** Primera Edición. Estándar publicado por International Organization for Standardization en Suiza en el año 2005.

ISO 7498-2 **“Information processing systems - Open Systems Interconnection - Basic Reference Model Part 2 Security Architecture”.** Primera Edición. Estándar publicado por International Organization for Standardization en Suiza en el año 1989.

United States Government Department of Defense **“Orange Book”.** Primera Edición Publicado por el Departamento de Defensa de los Estados Unidos en Estados Unidos en el año 1983 Disponible en: http://nsi.org/Library/Compsec/orangebo.txt

FIPS 200 **“Minimum Security Requirements for Federal Information and Information Systems”.** Desarrollado por el NIST. Publicado por el Departamento de Comercio de los Estados Unidos en los Estados Unidos en el año 2006. Disponible en: http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf

Francisco López Crespo, Miguel Angel Amutio Gómez, Javier Candau, José Antonio Mañas. **“Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información”.** Versión 2. Metodología publicada por el MINISTERIO DE ADMINISTRACIONES PÚBLICAS En España en el año 2006 Disponible en: http://www.csae.map.es/csi/pdf/magerit_v2/metodo_v11_final.pdf

CERT ® Coordination Center **“OCTAVE Method Implementation Guide”.** Versión 2. Metodología publicada por OCTAVE® Carnegie Mellon University en Estados Unidos en el año 2001. Disponible en: http://www.cert.org/octave/octavemethod.html

Gary Stoneburner, Alice Goguen, Alexis Feringa **“Risk Management Guide for Information Technology Systems”.** National Institute of Standards and Technology Publicación Especial 800-30. Metodología publicada por el Departamento de Comercio de los Estados Unidos en Estados Unidos en el año 2002.

Anexos

Anexo A. Retorno de la Inversión en la Seguridad Informática

Muchas empresas basan sus ventas de seguridad en el miedo, es decir, le exponen a las empresas casos donde los costos por no asegurar los sistemas son elevados o la imagen de la empresa es afectada seriamente y les mencionan que “eso” les puede ocurrir a ellos, donde “eso” es un incidente muy grave de seguridad cuyas consecuencias pueden ser graves a tal grado que ponen en peligro la existencia de la empresa.

Más que espantar a un cliente o al dueño de la empresa donde se labora para poder vender interna o externamente un proyecto de seguridad, es necesario crear la conciencia de las ventajas de incorporar seguridad para la empresa y el costo que supondrá no implementar ninguna medida de seguridad.

Crear conciencia en una empresa de la necesidad de la Seguridad Informática no es algo sencillo, la Seguridad Informática es vista como un mal necesario. Una de las principales dificultades es el hecho de que no existe un retorno de inversión claro, es decir, si una empresa decide invertir en TI poniendo en red a todos sus equipos para lograr así una mejor comunicación entre estos, a la larga obtendrá beneficios económicos, es decir, recuperará la inversión realizada y obtendrá una ganancia por encima de la inversión.

Desafortunadamente no ocurre lo mismo en el área de Seguridad, es un error pensar que la seguridad traerá un beneficio tradicional como un incremento de ventas o una reducción de costos. En el caso de la Seguridad Informática, el retorno de inversión se basa en calcular los costos ahorrados como consecuencia de evitar incidentes de seguridad o de mitigar los efectos de los incidentes en caso de que ocurran. En otras palabras, la seguridad es un elemento cuyo valor recae en la disminución de riesgos, lo cual incluso puede traer otro tipo de beneficios como bien pudiera ser la imagen de la empresa.

Normalmente una empresa va a tratar de reducir los costos y gastar sus recursos en soluciones que le van a traer un beneficio. Para poder mostrarle a una empresa el valor que aporta la seguridad habrá que darle a conocer los recursos que puede ahorrar implementando controles que mitiguen los riesgos de incidentes.

Para entenderlo mejor podemos usar a una empresa bancaria de ejemplo. Normalmente los bancos por ser instituciones que manejan grandes cantidades de dinero están expuestos a diferentes amenazas, logrando muchas de ellas causar pérdidas económicas al banco. Uno de los ataques más comunes sobre las instituciones bancarias es el *Phishing*, este tipo de ataque es un tipo de estafa donde el atacante se hace pasar por una institución bancaria y obtiene nombres de usuario y contraseñas de los clientes del banco mediante una página falsa en apariencia igual a la del banco, una vez obtenidos dichos datos los usa en la página real del banco y tiene acceso para realizar movimientos bancarios. En este tipo de ataque es principalmente perjudicado el cliente del banco, sin embargo, también es afectada la institución bancaria. Al termino del año este tipo de ataque significará un costo para las instituciones bancarias y sin embargo si se conoce el problema y se invierte en buscar soluciones de seguridad que mitiguen las consecuencias del *Phishing*, el porcentaje en que es disminuido el riesgo de sufrir un ataque de este tipo es la ganancia que significa invertir en la Seguridad Informática.

En este ejemplo queda claro que la seguridad tiene un costo, pero a su vez aporta un beneficio, el cual si bien no está dado en ganancias para la empresa, si aporta valor

disminuyendo las pérdidas que ocasiona el hecho de no tener seguridad.

Como se ha mencionado en el capítulo 4, las diferentes metodologías señalan la importancia de obtener el apoyo de la gerencia para realizar el Análisis de Riesgos. Los argumentos mencionados en este Anexo, si bien por si solos no lo obtendrán, si servirán de apoyo para obtener dicho apoyo, pues muestran el valor que tiene la Seguridad Informática.

Referencias Anexo A

Ernesto Pérez **“ROSI (Return on Information Security Investment)”** Página Web disponible en: http://pastorcortes.net/rosi_return_on_information_security_investment_ Leído por última vez el 2 de octubre de 2009.