UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

UNA METODOLOGÍA DE ANÁLISIS Y EVALUACIÓN DE RIESGOS EN TECNOLOGÍAS DE INFORMACIÓN

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

INGENIERO EN COMPUTACIÓN

PRESENTAN:

CRUZ MENDOZA JUAN CARLOS
JALPILLA JIMÉNEZ ROBERTO
RAMÍREZ SAN MIGUEL ESTEBAN

DIRECTOR DE TESIS:
ING. HERIBERTO OLGUÍN ROMO

CUIDAD UNIVERSITARIA
MÉXICO, D.F. 2014

"El mayor riesgo es no asumir ningún riesgo…
En un mundo que cambia realmente rápido,
la única estrategia en la que el fracaso
está garantizado es no asumir riesgos".

Mark Zuckerberg
(Filántropo de EE.UU)

Con todo mi cariño y mi amor para las personas que hicieron todo en la vida para que yo pudiera lograr mis sueños, por motivarme y darme la mano cuando sentía que el camino se terminaba, a ustedes por su paciencia y comprensión que prefirieron sacrificar su tiempo para que yo pudiera cumplir con el mío, por su bondad y sacrificio que me inspiraron a ser mejor para ustedes. Con todo mi cariño está tesis se las dedico a ustedes: Papá, Mamá y Hermanos.

Juan Carlos

Agradecimientos.

Le agradezco a Dios por acompañarme y guiarme a lo largo de mis estudios, por ser fortaleza en los momentos de debilidad y por brindarme una vida llena de aprendizajes, experiencias y sobre todo felicidad.

Le doy gracias a mis padres Elizabeth y Roberto por apoyarme en todo momento, por los valores que me han inculcado y por haberme dado la oportunidad de tener una excelente educación en el transcurso de mi vida. Sobre todo por ser un excelente ejemplo a seguir.
A mi hermana Claudia por ser parte importante de mi vida y representar la unidad familiar.

A mi director de tesis, Ing. Heriberto Olguín Romo por su esfuerzo y dedicación, quien con sus conocimientos, su experiencia, su paciencia y su motivación ha logrado la realización de esta tesis. En especial un profundo reconocimiento por su trayectoria como académico en la Facultad de Ingeniería, gracias por habernos compartido sus conocimientos y sobre todo su amistad.

A mi Alma mater, la UNAM que me brindó la oportunidad de formar parte de una de las mejores universidades del mundo y la mejor en Latinoamérica. Estoy muy orgullo de ser parte de esta gran familia.

A la Facultad de Ingeniería, la cual considero como una casa para mí, la que me dio una educación de alta calidad y no solo me formo como ingeniero si no también me hizo ser una mejor persona.

A mis sinodales Mtro. Juan José Carreón Granados, M.I. Adolfo Millán Nájera, M.I. Norma Elva Chávez Rodríguez y Dra. María Del Pilar Ángeles por tomarse la molestia de revisar esta tesis y apoyarme en los trámites para el examen profesional.

A mis compañeros de tesis: Esteban y Juan, por el apoyo.

Y finalmente quiero extender un sincero agradecimiento a Jenny Sotelo, Pamela Flores e Irma Dionisio de Grupo Financiero Inbursa por su comprensión y apoyo de permitirme terminar con los trámites para el examen profesional.

Son muchas las personas que han formado parte de mi vida profesional a las que me encantaría agradecerles su amistad, consejos, apoyo, ánimo y compañía en todos los momentos de mi vida. Algunas están aquí conmigo y otras en mis recuerdos y en mi corazón, sin importar en donde estén quiero darles las gracias por formar parte de mí y por todo lo que me han brindado, gracias.

Roberto Jalpilla

Agradecimientos.

A mi esposa, por su apoyo y amor incondicional; en todos los momentos difíciles que hemos pasado.

A todos aquellos que han aportado consciente o inconscientemente una parte de ellos para mi formación profesional, y crecimiento personal.

A nuestro director de tesis, Ing. Heriberto Olguín Romo; por toda su experiencia volcada en este trabajo.

A Roberto y Juan Carlos, por su amistad y apoyo.

Gracias a todos ellos, porque este es el resultado de su esfuerzo, amor y dedicación; pero sobre todo agradezco a mis padres por ser un ejemplo a seguir. Por mostrarme el camino correcto, y forzarme a seguirlo, haya o no querido.

Finalmente a mi Alma Mater, la Universidad Nacional Autónoma de México, y todos los profesores de la Facultad de Ingeniería por la formación académica, que de ellos recibí.

Esteban

UNA METODOLOGÍA DE ANÁLISIS Y EVALUACIÓN DE RIESGOS EN TECNOLOGÍAS DE INFORMACIÓN

MARZO 2014

Introducción

El avance acelerado al que se han enfrentado diversas organizaciones está estrechamente vinculado con el incremento en el uso de las tecnologías de información, así como la evolución en la forma de su utilización. Este progreso ha permitido que las Tecnologías de Información se conviertan en una herramienta trascendental para diseñar e implementar mejores y más efectivos procesos, generando oportunidades de crecimiento, así como la posibilidad de contar con información veraz y oportuna para una eficaz toma de decisiones. Sin embargo, esto conlleva a tener una dependencia en la información y en los sistemas que la proporcionan.

Este tipo de dependencia trae consigo una serie de riesgos inherentes que las organizaciones deben de enfrentar; a estas exposiciones se les conoce como riesgo tecnológico. Dicho riesgo es parte complementaria al riesgo operacional, el cual mientras exista este entorno, su gestión desempeñará un papel crítico y esencial dentro de las operaciones como factor de control estratégico.

La seguridad de la información es un concepto que se encuentra cada vez más inmerso en nuestra sociedad, principalmente en el uso extenso que le damos a la tecnología de las computadoras. En la vida diaria, trabajamos con computadoras, atendemos a clases o curso en línea, compramos todo tipo de mercancías en Internet, conversamos con familiares y amigos en todo el mundo a través de la red, con nuestra laptops revisamos correos desde cualquier lugar con red móvil; de igual forma mediante teléfonos inteligentes, revisamos el estado de nuestra cuenta bancaria a través de aplicaciones móviles, monitoreamos nuestro ejercicio físico mediante sensores y aplicaciones que se conectan a Internet, pudiendo compartir esta información de manera inmediata con una comunidad de cientos de miles de personas, y así podemos continuar *ad infinitum*.

Con los ejemplos indicados es fácil darse cuenta que la tecnología nos permite ser más productivos y estar en contacto con mayor número de personas, además de acceder, con unos cuantos ‘clicks’, a una gran cantidad de información que antes no hubiese sido posible; sin embargo, todo esto ocasiona un tipo diferente de riesgo que no se tenía con anterioridad. Por ejemplo, si nuestra cuenta bancaria es manipulada por un atacante cibernético, las consecuencias pueden ser funestas para nosotros; de inmediato podemos quedarnos sin fondos, al ser éstos transferidos a otra cuenta o a otro banco sin nuestro conocimiento, lo que además del daño personal, significa la pérdida de millones de dólares para el banco, al enfrentarse a demandas legales y sufrir daños en su reputación, todo esto a causa de un posible error en la configuración de sus sistemas de información, que pudieron permitir el ingreso de atacantes a las bases de datos que contienen información confidencial. Con mayor frecuencia estas noticias son comentadas en los medios de comunicación, lo que no sucedía hace 30 años cuando eran prácticamente inexistentes, debido a la tecnología de la época y la cantidad reducida de gente que la usaba.

La seguridad de la información es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma.

El concepto de seguridad de la información no debe ser confundido con el de seguridad informática, ya que este último sólo se encarga de la seguridad en el medio informático, pero la información puede encontrarse en diferentes medios o formas y no sólo en medios informáticos. Para el hombre como individuo, la seguridad de la información tiene un efecto significativo respecto a su privacidad, la que puede cobrar distintas dimensiones dependiendo de la cultura del mismo.

El campo de la seguridad de la información ha crecido y evolucionado considerablemente a partir de la Segunda Guerra Mundial, convirtiéndose en una carrera acreditada a nivel mundial. Este campo ofrece muchas áreas de especialización, incluidos la auditoría de sistemas de información, planificación de la continuidad del negocio, ciencia forense digital y administración de sistemas de gestión de seguridad, para nuestro caso la especialidad en el análisis y evaluación de riesgos en tecnologías de información, entre otros.

De manera general, la seguridad de la información significa cuidar nuestros activos. Esto es protegernos de los atacantes que invaden nuestras redes, desastres naturales, condiciones ambientales adversas, fallas en el suministro de energía, robo o vandalismo, u otro estado no deseable. Al final, intentamos asegurarnos de cualquier forma indeseable de ataque.

Los sistemas y la información que éstos guardan debe ser protegida y preservada, para ello es necesario hacer un estudio real de las amenazas y de las formas en que las mismas pueden ser reducidas, por esta razón, el presente trabajo tiene como una de sus metas primordiales el orientar, sobre los aspectos importantes que se deben considerar en un Análisis y Evaluación de Riesgos en Tecnologías de Información de cualquier empresa o institución.

Sin embargo, al procurar la protección a nuestra información también debemos considerar hasta dónde se debe llegar en la búsqueda de dicha protección. El tener el equipo o sistema donde nuestra información reside, aislado dentro de una bóveda de seguridad y con guardias armados, podemos tener la certeza, hasta cierto punto; que nuestra información está resguardada; pero esto hace inoperante e inútil, tanto la información almacenada en dicho sistema, como el sistema mismo. Es por esto necesaria una evaluación de los riesgos de seguridad a los que cada empresa está expuesta; así como su correcta mitigación de acuerdo a los resultados obtenidos en el análisis de los datos recolectados durante las diferentes fases del proyecto de evaluación de riesgos de seguridad, que debe ser aplicado a todo tipo de entidades que manejen Tecnologías de Información a cualquier nivel.

Debido a la trascendencia de los controles de seguridad y contramedidas que ameriten ser implementadas en la mitigación de los riesgos, este trabajo pretende enfatizar la importancia y significado de una Metodología de Análisis y Evaluación de Riesgos en Tecnologías de Información, por ello se ha bosquejado una temática amplia y diversa en un lenguaje sencillo que resalta el qué y cómo se debe hacer.

En el primer capítulo se revisa la evolución de las Tecnologías de Información, los tipos de tecnologías y la necesidad de un análisis y evaluación de los riesgos en las mismas.

En el capítulo dos se presenta el marco conceptual de los riesgos, dejando claros los conceptos, los tipos de causas de riesgos y los procesos para la inicialización del análisis de éstos.

El tercer capítulo trata de metodologías existentes para una evaluación de riesgos en Tecnologías de Información.

En el capítulo cuatro se han considerado las normas y estándares internacionales en el tratamiento de riesgos en Tecnologías de Información, así como políticas y procedimientos necesarios para las empresas o instituciones.

El quinto capítulo contempla el desarrollo de “Una metodología de análisis y evaluación de riesgos en Tecnologías de Información”, identificando los riesgos y detectando las principales áreas de recolección de datos, para su análisis y evaluación, así como las recomendaciones respectivas.

El objetivo principal del presente trabajo es que, tanto los alumnos de la licenciatura de Ingeniería en Computación, como los profesionales en Tecnologías de Información, cuenten con elementos que les permitan analizar y evaluar los riesgos, de esta manera fundamentar la reducción y posible eliminación de los mismos.

ÍNDICE

CAPÍTULO 1

ANTECEDENTES

CAPÍTULO 1

ANTECEDENTES

1.1. Evolución de las tecnologías de información

Los adelantos en el campo de las Tecnologías de Información en los últimos 30 años, han cambiado extraordinariamente la manera en cómo trabajan las personas, de tal forma que han permitido automatizar de forma gradual las tareas que anteriormente eran realizadas tediosamente por operadores u oficinistas. La velocidad de esta evolución en pocos años ha producido además de beneficios, modificaciones en la forma y tiempo de trabajo en las organizaciones.

La necesidad de información es tan antigua como el ser humano, pero no es hasta mediados del siglo XIX cuando se muestran los reales avances tecnológicos. La historia nos muestra desde el singular sistema de comunicación que empleaba antorchas sobre torres distantes; la transmisión de símbolos y letras del alfabeto griego cerca del siglo 300 a.c., hoy en día con la creación de la computadora y posterior-mente la aparición de Internet se amplió el acceso a la información permitiendo la comunicación casi instantánea con todo el mundo.

Así mismo la introducción de las nuevas tecnologías en los negocios y en el hogar han cambiado la organización y el funcionamiento de todo tipo de empresas e instituciones, proporcionando mejores métodos de búsqueda y acceso a la información, además de herramientas para el óptimo manejo de recursos.

Sin embargo debido al constante cambio e innovación, algunas tecnologías se hacen rápidamente obsoletas, por lo que obliga a las organizaciones a adquirir tecnología que se ajuste a sus estrategias, infraestructura y procesos de negocio.

Es por eso que las Tecnologías de Información han obtenido una relevancia estratégica, debido a que cambian la forma en que operan las organizaciones.

Hoy en día la integración de la computación, las telecomunicaciones y las técnicas para el procesamiento de datos son los principales protagonistas para el desarrollo informático, los principales factores para esto son:

- La microelectrónica por el avance en la velocidad y capacidad de procesamiento en las computadoras.
- Las telecomunicaciones en el amplio desarrollo de las redes con alcance local y global.
- El desarrollo de programas y aplicaciones para los usuarios, provocando un ambiente amigable con el uso de técnicas multimedia.

Durante mucho tiempo, la función de la informática en las empresas fue considerada como parte de las herramientas operativas con las que contaba la organización, pero hoy en día las Tecnologías de Información son consideradas como áreas de oportunidad para lograr objetivos y ventajas en el desarrollo de los negocios, ya que se han convertido en el corazón de las operaciones de cualquier organización, desde sistemas transaccionales que ayudan en las operaciones diarias hasta las aplicaciones que contribuyen a tomar decisiones gerenciales definiendo el rumbo de la organización.

Actualmente las organizaciones que tengan la información precisa en el momento que sus ejecutivos la requieran, contarán con un elemento muy importante para la toma de decisiones, lo que les permitirá contar con una ventaja competitiva respecto a sus competidores.

1.2. Tipos de tecnología

Con base en las tecnologías que han cambiado en la forma de operar en las organizaciones, se definen los siguientes tres tipos:

1.2.1. Tecnología aplicable

A medida que transcurre el tiempo las Tecnologías de Información han ido evolucionando en su uso; en sus inicios se utilizaban para tareas rutinarias siendo muy costosas y además eran consideradas como un gasto extra para la organización, pero al paso del tiempo empezaron a realizar tareas más complejas y completas; integrando en gran parte las actividades de la organización; hoy en día, las posibilidades que las TI nos dan, es la de ser en sí mismas la ventaja competitiva del negocio, considerandose como un activo más para las organizaciones y no un costo adicional.

Por lo tanto, las TI juegan también un papel importante, no sólo como herramientas de implementación de módulos del Sistema de Información (SI), sino por las oportunidades que por sí mismas abre a las empresas.

1.2.2. Tecnología necesaria

Podemos decir que la tecnología está siempre en función de los objetivos estratégicos que persigue el negocio, es decir, que al escoger entre las tecnologías sobre las cuales invertir, una organización debe basar sus decisiones en un profundo conocimiento de cada tecnología importante en sus actividades y no en simples indicadores como la oferta del mercado actual.

Según Michael Porter: “De todas las cosas que pueden cambiar las reglas de competencia, el cambio tecnológico está entre las más prominentes.” Pero el uso de las Tecnologías de Información no es importante por sí mismo, es importante si trae consigo el logro de una ventaja competitiva.

Podemos afirmar que las tecnologías necesarias en la empresa, son aquellas que contribuirán al máximo en el logro de los objetivos estratégicos del negocio.

1.2.3. Tecnología deseada

El utilizar una nueva tecnología implica cambios, ya que en muchas ocasiones no será posible hacer lo mismo que antes y de la misma manera, sólo que se utilizará una tecnología diferente. Debemos estar conscientes de los cambios que el uso de nuevas herramientas implica. Tener en cuenta las características de la tecnología que estamos usando y de la nueva, volviendo a considerar el funcionamiento para que el Sistema de Información proporcione los resultados deseados.

Por lo tanto, el uso de las nuevas tecnologías a menudo no es deseado por parte del personal, que deben sacrificar las "viejas formas de hacer las cosas" para aceptar los cambios que éstas traen consigo. Los empleados deberán estar dispuestos al cambio, interesarse en aprender y querer trabajar con las nuevas tecnologías. Es importante el papel del líder para crear las condiciones idóneas para que esto suceda.

1.3. Necesidad del control de Tecnologías de Información

En la actualidad las organizaciones son más dependientes de sus redes informáticas, y un problema que las afecte, por pequeño que sea, puede llegar a comprometer la continuidad de las operaciones, situación que inevitablemente se traduce en pérdidas económicas, retraso en las operaciones y crisis de confianza por parte de los usuarios.

Sumado a lo anterior se encuentra la ausencia de una adecuada política de seguridad de las redes. Este es un problema que está presente por el solo hecho de subestimar las fallas que a nivel interno se producen, considerando sobre todo que la propia complejidad de la red es una dificultad para la detección y corrección de múltiples y variados problemas de seguridad que deben ser detectados.

Los problemas o las fallas de los sistemas informáticos ocasionan graves crisis empresariales, daños en la reputación causados por suplantaciones de identidad, pérdidas en el negocio por fallas en los sistemas, así como restricciones normativas que surgen por temas derivados del no cumplir con las políticas establecidas.

Recientemente, hemos podido ver algunas noticias sobre historias relacionadas con riesgos en Tecnologías de Información, éstos incluyen: ataques de phishing, robo de datos confidenciales, suplantaciones de identidad, robo de cintas con copias de seguridad, pleitos derivados de un deficiente mantenimiento y backup de registros electrónicos y problemas derivados de la propiedad intelectual, entre otros.

1.4. La realidad de la gestión de riesgos en Tecnologías de Información

La mayoría de las empresas e instituciones públicas y privadas tienen un limitado conocimiento de los peligros que corren sus Sistemas de Información; no explotan en su totalidad la amplia gama de herramientas que existen para gestionar riesgos y tampoco han comenzado a implementar los conocimientos y los procesos necesarios para esta gestión.

1.5. El análisis y la evaluación de los riesgos

El avance tecnológico ha traído consigo un reto mayor para quienes se dedican a combatir programas con características maliciosas, la difusión de nuevas técnicas y metodologías de ataques y amenazas informáticas; cada vez más sofisticadas y eficaces dificultan la buena marcha de las organizaciones. No es un secreto la cantidad de recursos que invierten las empresas para evitar intromisiones y manipulaciones que pongan en riesgo, desde la integridad de los datos hasta las operaciones propias de la entidad.

Una vez que los riesgos han sido identificados el administrador de riesgos debe evaluarlos. El paso a seguir es hacer el análisis y la valoración. En esta actividad se tiene como objetivo, una vez registrados los riesgos, la determinación y cálculo de los parámetros que, con posterioridad, nos facilitarán la evaluación de los riesgos.

Como procedimiento a seguir se identificarán las variables específicas y se analizarán los factores obtenidos. Los criterios de análisis del riesgo, que usaremos para este caso en particular son: probabilidad o frecuencia, gravedad o impacto y la aceptación del riesgo.

Para poder hacer el análisis y la evaluación es necesario elaborar las escalas de probabilidad y gravedad en que se pueden presentar las amenazas. Estas dos tablas tienen como finalidad obtener una calificación del riesgo en cuanto a frecuencia o posibilidad de ocurrencia y en cuanto a la consecuencia o gravedad, si se llegara a materializar la amenaza.

Ambas escalas son generadas por los responsables del proceso y de la tecnología informática en forma estándar para la empresa o el proyecto, ya que las consecuencias de un determinado evento o amenaza es diferente para cada situación.

El término probabilidad se refiere a la posibilidad de ocurrencia (frecuencia) que puede tener el riesgo evaluado; a los valores o niveles de probabilidad se asigna un valor relativo (cualquiera); generalmente por facilidad de manejo se utilizan valores enteros. Ver ejemplo en tabla 1.1. Ejemplo para una escala de probabilidad de riesgo.

Valor	Probabilidad	Definición
1	Improbable	Se presenta bajo circunstancias extremas de orden público en el país, de catástrofe o bajo situaciones excepcionales fuera del alcance de la organización o del proyecto. Como paros, huelgas, sabotajes o amenazas de terrorismo.
2	Remoto	Se presenta por situaciones atribuibles a las personas, y pueden ser causadas por hechos internos de la organización hacia el proyecto como suspenderlo, no apoyarlo, abortarlo, entre otras.
3	Ocasional	El evento se clasifica como no-rutinario y no inherente a la tecnología. Su frecuencia se asocia con variables externas a la tecnología, los procesos o componentes del proyecto.
4	Moderado	Se presenta por situaciones atribuibles al descuido o error humano que afectan la ejecución del proyecto.
5	Frecuente	Se presenta con cierta regularidad, y su causa es atribuible a los recursos mínimos del proyectos (personas, presupuesto, tiempo, tecnología) los cuales son necesarios para su ejecución.
6	Constante	Se presenta en el día a día, su origen es atribuible a situaciones normales del proyecto como interrupciones menores de los procesos, los servicios de tecnología, la desviación de los recursos y otros similares.

Tabla 1.1. Ejemplo para una escala de probabilidad de riesgo.

Después de revisar los diferentes métodos, metodologías y herramientas existentes, se propone el esquema que se describe en la figura 1.1. Esquema del análisis y evaluación de riesgo, para llevar a cabo el mencionado análisis y evaluar su riesgo.

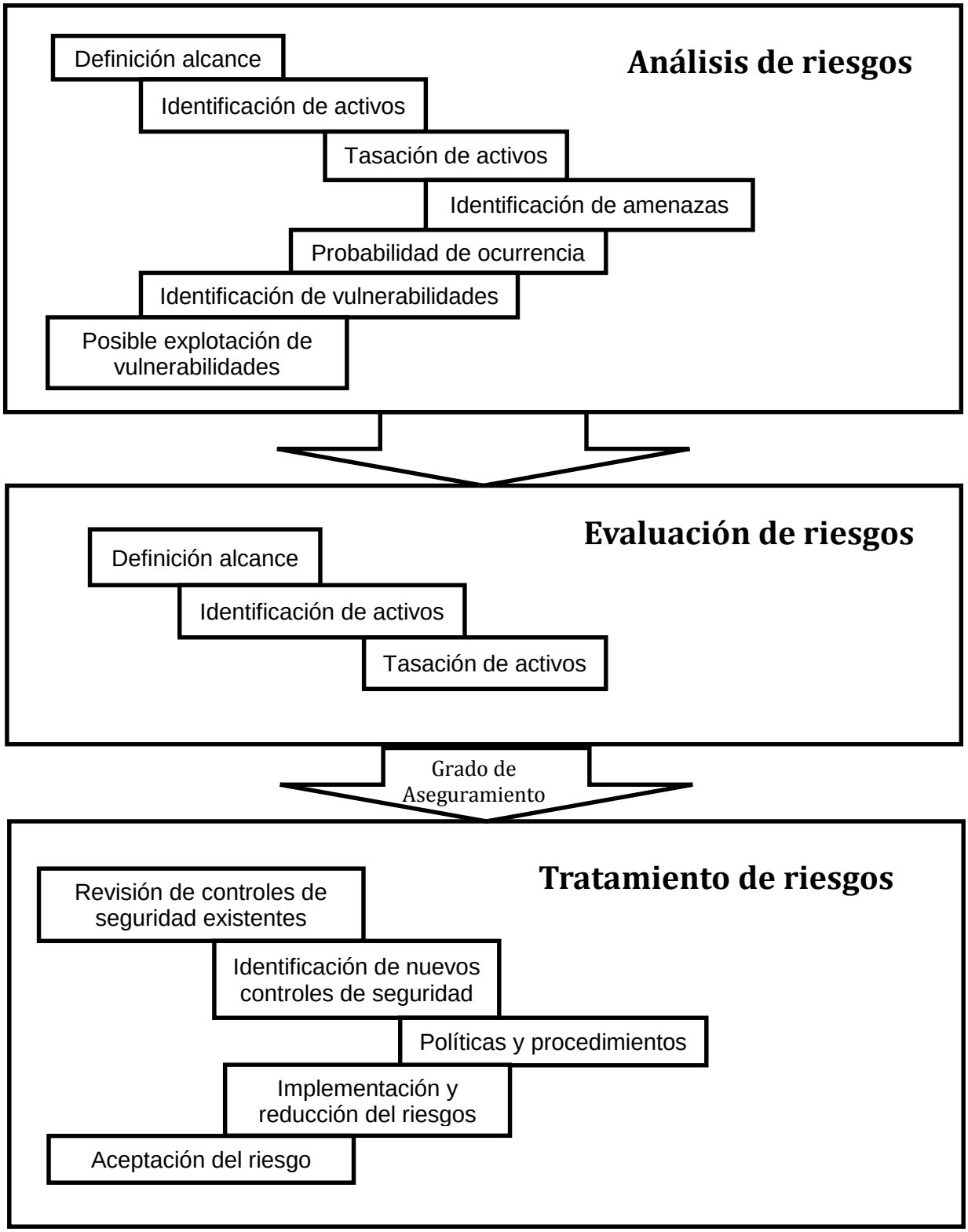


Figura 1.1. Esquema del análisis y evaluación de riesgo.

Una metodología recomienda que para llevar a cabo una evaluación de riesgos, se defina primero el alcance del proyecto y con base en ello, identificar todos los activos de información. Éstos deben ser tasados para identificar su impacto en la organización, estipulando qué activos están bajo riesgo y con base en ello; poder tomar decisiones en relación a qué riesgos aceptará la organización y qué controles serán implantados para mitigarlo.

A la organización le corresponderá revisar los controles implantados a intervalos de tiempo regular, para asegurar su ajuste, eficacia y que de esta forma se controlen los niveles de riesgos aceptados y el estado del riesgo residual (es el riesgo que queda después del tratamiento del mismo).

CAPÍTULO 2

MARCO TEÓRICO: RIESGOS EN TECNOLOGÍAS DE INFORMACIÓN

CAPÍTULO 2

MARCO TEÓRICO:
RIESGOS EN TECNOLOGÍAS DE INFORMACIÓN

2.1. Fundamentación teórica

Conceptos de riesgo:
Riesgo se refiere a la incertidumbre o probabilidad de que ocurra o se realice un evento, el cual puede ser previsto; en este sentido podemos decir que el riesgo es la contingencia de un daño.

José Salvador Sánchez define el riesgo como cualquier elemento potencial que puede provocar resultados no satisfactorios en el desarrollo de un proyecto.

Riesgo es también toda aquella eventualidad que imposibilita el cumplimiento de un objetivo. De manera cuantitativa el riesgo es una medida de las posibilidades de incumplimiento o exceso del objetivo planeado. Así definido, un riesgo conlleva a dos tipos de consecuencias: ganancias o pérdidas.

2.2. Clasificación de riesgos

No existe una clasificación oficial de los riesgos; se pueden clasificar en función de diferentes parámetros. A pesar de la dificultad de clasificación, una posible puede estar en función de los siguientes parámetros:

- *Parámetros de vulnerabilidad*: la capacidad de los riesgos de afectar o no a grandes colectivos. Ejemplos de riesgos colectivos son las inundaciones, los terremotos, las emergencias de tipo químico en industrias, etc. Y riesgos no colectivos serían tales que su materialización nunca supondrá una afectación importante de personas y normalmente se limita a una única persona o a un número muy limitado.

- *Parámetros temporales*: si los efectos de los riesgos son o no inmediatos. Los riesgos pueden ser eventuales o puntuales si sus efectos son inmediatos, tales como: sismos, incendios forestales, escapes químicos y otros; mismos que requieren una respuesta inmediata para minimizar sus consecuencias.

- Parámetros socioeconómicos y medioambientales. El origen de los riesgos considerados colectivos y eventuales, es decir, el medio en el que se inician y las causas que los generan.

Con objeto de ubicarnos en los tipos de riesgos de Tecnologías de Información en las organizaciones, enunciaremos algunos de los más comunes.

2.2.1. Riesgo de negocio

Es una circunstancia o factor que puede tener un impacto negativo o positivo sobre el funcionamiento o la rentabilidad de una empresa determinada. En ocasiones se refiere como el riesgo de la empresa. El riesgo de negocio puede ser el resultado de las condiciones internas, así como algunos factores externos que pueden estar presentes en la comunidad empresarial en general.

2.2.2. Riesgo inherente

Este tipo de riesgo tiene que ver exclusivamente con la actividad económica o giro empresarial del negocio, independientemente de los sistemas de control interno que se estén aplicando.

2.2.3. Riesgo de control

Este tipo de riesgo considera de manera muy importante a los sistemas de control interno que estén implementados en la empresa, y que en ciertas circunstancias lleguen a ser insuficientes o inadecuados para la aplicación y detección oportuna de irregularidades. Es por ello que una administración debe tener constante revisión, verificación y ajustes en los procesos de control interno.

2.2.4. Riesgo estratégico

El riesgo estratégico es la forma de competir y la relación con el entorno, así como las tensiones organizacionales internas, que representan barreras para poder ejecutar la estrategia seleccionada con éxito. Se asocia con la forma en que se administran las empresas e instituciones. El manejo del riesgo estratégico se enfoca a asuntos globales relacionados con el cumplimiento de la misión de la organización,

2.2.5. Riesgo operativo

Se puede definir como el riesgo de que se presenten pérdidas por fallas en los sistemas administrativos y procedimientos internos, así como por errores humanos, intencionales o no.

2.2.6. Riesgo financiero

Se define como la posibilidad de deterioro o perdida derivada de la realización de operaciones financieras que pueden afectar a la capitalización bursátil o valor de mercado de la empresa.

2.2.7. Riesgo de cumplimiento

Se asocia con la capacidad de la empresa para cumplir con los requisitos regulativos, legales, contractuales, de ética pública, participación, servicio a la comunidad, interacción con el ciudadano, respeto a los derechos, a la individualidad, la equidad y la igualdad.

2.2.8. Riesgo de tecnología

Se asocia con la capacidad de la empresa en que la tecnología disponible satisfaga las necesidades actuales y futuras de la empresa, soportando el cumplimiento de la misión.

2.2.9. Riesgo profesional

Se define como una situación potencial de peligro ligada directa o indirectamente al trabajo y que puede materializarse con el daño profesional.

Con esta definición se puntualiza que no siempre el riesgo profesional conduce al daño profesional, es decir puede existir riesgo sin producirse daño.

2.3. Tipos de causas de riesgos

Las causas de riesgo más comunes, para efectos dentro de las tecnologías de información, se dividen en: externas e internas.

Las causas de riesgo externas pueden ser de dos clases: naturales y originadas por el hombre.

Las causas de riesgo naturales son habitualmente las siguientes:

- Temblores
- Inundaciones
- Tornados
- Huracanes
- Tormentas eléctricas
- Erupciones volcánicas

Las causas de riesgo originadas por el hombre, son entre otras, las siguientes:

- Incendios
- Explosiones
- Accidentes laborales
- Daños mal intencionados
- Sabotaje
- Robo
- Fraude

Las causas de riesgo internas, se derivan a partir de las mismas empresas. Son más frecuentes las causas internas de riesgo que las externas.
Entre las causas de riesgo internas tenemos básicamente:

- Robo de materiales, monetario y de información.
- Sabotaje.
- Suplantación de identidades.
- Falta de recursos económicos.
- Destrucción o alteración de datos y de recursos.
- Personal no capacitado.
- Fraude interno y externo.
- Ausencia de seguridad física, tanto en la empresa como de su información.
- Venta de información de la empresa a la competencia.

Adicional a los ataques intencionados, se encuentra el uso incorrecto de la tecnología, que en muchas ocasiones es la mayor causa de vulnerabilidad y los riesgos a los que se exponen las organizaciones.

2.4. Riesgos en Tecnologías de Información

2.4.1. Concepto de riesgo

El concepto de riesgo en Tecnologías de Información puede definirse como el efecto de una causa multiplicado por la frecuencia probable de ocurrencia dentro del entorno de las TI. Surge así, la necesidad del control que actúe sobre la causa del riesgo para minimizar sus efectos. Cuando se dice que los controles minimizan los riesgos, lo que en verdad hacen es actuar sobre las causas de los riesgos, para minimizar sus efectos.

2.4.2. Valoración del riesgo

La valoración del riesgo consta de tres etapas: la identificación, el análisis y la determinación del nivel del riesgo. Para cada una de ellas es necesario tener en cuenta la mayor cantidad de datos disponibles, como los planes de mejoramiento, así como contar con la participación de las personas que ejecutan los procesos y procedimientos para lograr que las acciones determinadas alcancen los niveles de efectividad esperados.

2.4.3. Identificación del riesgo

El proceso de identificación del riesgo debe ser permanente, integrado al proceso de planeación y responder a las preguntas del: ¿qué?, ¿cómo? y ¿por qué se pueden originar hechos que influyen en la obtención de resultados?.

Una manera de realizar la identificación del riesgo es a través de la elaboración de un mapa de riesgos, el cual como herramienta metodológica permite hacer un inventario de los mismos en forma ordenada y sistemática, definiendo en primera instancia los riesgos, posteriormente presentando una descripción de cada uno de ellos y sus posibles consecuencias. Un mapa de riesgos puede ser el que se muestra en la tabla 2.1.

RIESGO	DESCRIPCIÓN	POSIBLES CONSECUENCIAS
Posibilidad de ocurrencia de aquella situación que pueda entorpecer el normal desarrollo de las funciones de la entidad y le impidan el logro de sus objetivos.	Se refiere a las características generales o las formas en que se observa o manifiesta el riesgo identificado.	Corresponde a los posibles efectos ocasionados por el riesgo, los cuales se pueden traducir en daños de tipo económico, social, o administrativo, entre otros.

Tabla 2.1. Un mapa de riesgos

2.5. Análisis de riesgos

El objetivo del análisis de riesgos es establecer una valoración y priorización de los riesgos con base en la información ofrecida por los mapas elaborados en la etapa de identificación, con el fin de clasificar los riesgos y facilitar información para establecer el nivel de riesgo, así como las acciones que se van a implementar.

Se han establecido dos aspectos para realizar el análisis de los riesgos identificados:
Aspecto probabilístico: La posibilidad de ocurrencia del riesgo, la cual puede ser medida con criterios de frecuencia o teniendo en cuenta la presencia de factores internos y externos que puedan propiciar el riesgo, aunque éste no se haya presentado nunca.

Para el análisis cualitativo se establece una escala de medida cualitativa en donde se definen unas categorías a utilizar y la descripción de cada una de ellas, con el fin de que cada persona la aplique; por ejemplo:

Alta: Es muy factible que el hecho se presente.

Media: Es factible que el hecho se presente.

Baja: Es poco factible que el hecho se presente.

Aspecto de impacto: Consecuencias que puede ocasionar a la organización la materialización del riesgo.

El diseño anterior puede aplicarse para la escala de medida cualitativa de impacto, estableciendo las categorías y la descripción; por ejemplo:

Alto: Si el hecho llegara a presentarse, tendría alto impacto o efecto sobre la entidad.

Medio: Si el hecho llegara a presentarse tendría medio impacto o efecto en la entidad.

Bajo: Si el hecho llegara a presentarse tendría bajo impacto o efecto en la entidad.

2.5.1. Definición de alcance

El primer paso, con base en la metodología que se propone en el capítulo 5, es evaluar la seguridad física y lógica de la empresa.

La seguridad física tiene como finalidad:

- Establecer seguridades en los accesos de entrada y salida a la empresa y por consiguiente al departamento de sistemas.
- Establecer respaldos actualizados de la información (bases de datos) que tiene el departamento y mantenerlos en sitios alternos seguros.
- Contratar un seguro, de manera que los equipos puedan ser remplazados.

La seguridad lógica tiene como finalidad:

- Mantener la confiabilidad, confidencialidad e integridad de la información de la empresa, mediante la utilización de métodos y procedimientos apropiados.
- Establecer claves de acceso, mediante algún software de seguridad existente en el mercado o desarrollado por la empresa.

2.5.2. Identificación de activos

Los activos son recursos del sistema de información o relacionados con él, necesarios para el correcto funcionamiento de la organización. Los activos pueden estructurarse en cinco categorías:

a. El entorno del sistema de información:
   - Equipamientos y suministros (energía regulada, condiciones ambientales, comunicaciones).
   - Recursos humanos de dirección, operación, desarrollo, otro.
   - Otros tangibles: edificios, mobiliario, instalaciones físicas, vehículos.

b. El sistema de información:
   - Hardware de proceso, almacenamiento, interfaces, otros.
   - Software de base, paquetes, producción de aplicaciones, modificación de firmware.
   - Comunicaciones: redes propias, servicios, componentes de conexión, etc.

c. Datos propiedad de la empresa y la información derivada.

d. Funcionalidades de la organización:
   - Objetivos y misión de la organización
   - Bienes y servicios producidos
   - Personal, usuarios y destinatarios de los bienes o servicios producidos

e. Otros activos no relacionados con los niveles anteriores:
   - Credibilidad: ética, jurídica, etc., o buena imagen de una persona jurídica o física.
   - Conocimiento acumulado.
   - Independencia de criterio de actuación.
   - Integridad de las personas, etc.

Además de identificar e inventariar los activos en cada uno de los anteriores niveles, deberemos fijar el estado de seguridad de cada activo en función de los siguientes atributos (tomando en cuenta un punto de vista cuantitativo):

Valuación de costos- Se basa en el valor del activo para ser reemplazado.
Valuación del mercado- Se toma el valor del activo en el mercado.
Valuación del ingreso- Tasa el valor del activo en el ingreso esperado de dicho activo.

El atributo tendrá los niveles: bajo, normal, alto o crítico, en función del nivel requerido.

- Confidencialidad de la información del activo.
  - Libre, sin restricciones en su difusión.
  - Restringida, con restricciones normales.
  - Protegida, con restricciones altas.
  - Confidencial, no de difusión por su carácter crítico.

- Integridad del activo. Facilidad mayor o menor de reobtener el activo con calidad suficiente.
  - Bajo, si se puede reemplazar fácilmente con un activo de igual calidad.
  - Normal, si se puede reemplazar con un activo de calidad semejante con una molestia razonable.
  - Alto, si la calidad necesaria es difícil y costosa de reconstruir.
  - Crítico, si no puede volver a obtenerse una calidad semejante.

- Disponibilidad del activo. Tiempo máximo de carencia del activo sin que las consecuencias o impactos sean graves para la organización.
- Menos de una hora, considerado como fácilmente recuperable.
- Hasta un día laborable, contando para la recuperación con ayuda telefónica de especialistas externos o de reposición con existencia local.
- Hasta una semana, contando para la recuperación con ayuda presencial de especialistas externos.
- Más de una semana, considerado como interrupción catastrófica.

2.5.3. Identificación de amenaza

Una vez que conocemos los recursos que debemos proteger es el momento de identificar las vulnerabilidades y amenazas que los afectan. Definimos como una vulnerabilidad a cualquier situación que pueda desembocar en un problema de seguridad y como una amenaza a un evento con un impacto indeseable en los activos de la organización, siendo los dos componentes de la amenaza, el agente que provoca la amenaza y el evento indeseable. Entre ambas existe una estrecha relación: "sin vulnerabilidades no hay amenazas y sin amenazas no hay vulnerabilidades".

Dada la importancia de las amenazas y del impacto que puede tener para la información de las organizaciones podemos clasificarlas en tres grupos.

- *Amenazas naturales:* condiciones de la naturaleza y la intemperie que podrán causar daños a los activos, tales como fuego, inundación, terremotos.
- *Amenazas intencionales:* son deliberadas, fraudes, vandalismo, sabotajes, espionaje, invasiones y ataques, robos y hurtos de información, entre otras.
- *Amenazas involuntarias*: son resultantes de acciones inconscientes de usuarios, por virus electrónicos, muchas veces causadas por la falta de conocimiento en el uso de los activos, tales como errores y accidentes.

Entre las principales amenazas, la ocurrencia de virus, la divulgación de contraseñas y la acción de hackers están entre las más frecuentes. A continuación se presenta una lista parcial de amenazas:

- *Fraude y robo:* afectan a los activos de valor.
- *Errores y omisiones*: dar lugar a la falta de datos y la integridad del sistema, la falta de estabilidad del sistema e incluso la divulgación de información confidencial.
- *Sabotaje:* incluir daño físico a las instalaciones o equipos, la eliminación intencionada de datos y la pérdida de integridad de los mismos.
- *Pérdida de Infraestructura:* en esta categoría incluir la interrupción del suministro de energía, tormentas invernales, huelgas laborales y ataques terroristas.
- *Espionaje:* robo de información exclusiva.
- *Código malicioso:* incluyen virus, troyano, gusano software que no funciona como se espera.
- *Confidencialidad de los datos*.

La existencia de amenazas está relacionada con la presencia de elementos que perjudican el uso adecuado de la información y del medio en que la misma información se está utilizando. De lo anterior se deriva otro objetivo de la seguridad de la información, éste es: la corrección de vulnerabilidades existentes en el ambiente en que se usa la información, a fin de reducir los riesgos a que está sometida, evitando así la concretización de una amenaza.

2.5.4. Probabilidad de ocurrencia

La probabilidad de ocurrencia de una amenaza es el número de probables incidentes que pudiese sufrir un activo expuesto sin ningún tipo de contramedida para defenderlo. Es importante señalar, que no todas las amenazas tienen la misma probabilidad de ocurrencia. Existen amenazas cuya frecuencia es baja y otras con frecuencia alta.

Con el fin de establecer una probabilidad o una estimación de la ocurrencia de un evento, los siguientes factores deben ser tomados en cuenta:

- Fuente de la amenaza y su capacidad.
- Naturaleza de la vulnerabilidad.

La probabilidad de que una vulnerabilidad potencial pueda ser explotada por una fuente de amenaza se puede clasificar como: alta, media-alta, media, media-baja y baja, como se describe a continuación.

Nivel	Definición
Alta = 5	La amenaza es altamente motivada y es suficientemente capaz de llevarse a cabo.
Media - alta = 4	La amenaza es fundamentada y es posible.
Media = 3	La amenaza es posible.
Media – baja = 2	La amenaza no posee suficiente capacidad de llevarse a cabo.
Baja = 1	La amenaza no posee la suficiente motivación y capacidad de llevarse a cabo.

2.5.5. Identificación de vulnerabilidades

Una vulnerabilidad es un error que representa un problema potencial, es decir, una condición de debilidad que le permite a una amenaza producir un daño a la organización.

Los grupos de vulnerabilidades los podemos identificar como:

- *Vulnerabilidades físicas*: por ejemplo instalaciones inadecuadas del espacio de trabajo, ausencia de recursos para la extinción de incendios; instalaciones eléctricas y de red deficientes, ausencia de identificación de personas y de lugares, entre otros. Estos puntos débiles, al ser explotados por amenazas, afectan directamente los principios básicos de la seguridad de la información, principalmente la disponibilidad.
- *Vulnerabilidades naturales:* Los puntos débiles naturales son aquellos relacionados con las condiciones de la naturaleza que pueden colocar en riesgo a la información.
- *Vulnerabilidades de hardware:* posibles fallas o defectos en la fabricación o configuración de los equipos de la empresa que pudieran permitir el ataque o alteración de la información. Existen muchos elementos que representan puntos débiles de hardware, por ejemplo: la ausencia de actualizaciones conforme a los programas de los fabricantes y conservación inadecuada de los equipos
- *Vulnerabilidades de software*: La configuración e instalación indebidas de los programas de computadora, que podrán llevar al uso inadecuado de los recursos por parte de usuarios mal intencionados, así como la ausencia de actualizaciones y programación insegura, etc.
- *Vulnerabilidades de medios de almacenamiento*: pueden ser afectados por puntos débiles que los dañen e incluso dejarlos inutilizables. Entre estos puntos débiles, destacamos los siguientes: tiempo de garantía y caducidad, defecto de fabricación, uso incorrecto, almacenamiento en condiciones no controladas, magnetismo, estática, moho, entre otros.
- *Vulnerabilidades de comunicación:* Cualquier falla en la comunicación que genere que la información quede no disponible para sus usuarios, o por el contrario, estar disponible para quien no posee autorización de acceso. La información sea alterada en su estado original, afectando su integridad; así mismo, la seguridad de la información también está asociada con el desempeño de los equipos involucrados en la comunicación.
- *Vulnerabilidades humanas:* Esta categoría está asociada con los daños que las personas pueden causar a la información y al ambiente tecnológico que la soporta.

2.5.6. Posible explotación de vulnerabilidades

Una amenaza, para poder causar algún tipo de daño a un activo de la empresa, tendría que explotar la vulnerabilidad del sistema, aplicación o servicio. Las vulnerabilidades son condiciones que pueden permitir que las amenazas las exploten y causen daño.

Una vez clasificadas las vulnerabilidades más críticas, se debe efectuar una prueba sobre ellas con el fin de realizar su explotación. El proceso de explotación debe incluir el escalar privilegios con el fin de tomar control total de los sistemas y de este modo seguir de manera estricta la forma en que se llevan a cabo los ataques en la vida real.

Una vez efectuadas las pruebas, considerando las anteriores recomendaciones, se debe tener una reunión técnica para informar de estos resultados, realizar una revisión general de las vulnerabilidades encontradas y la clasificación realizada; en esta reunión deben participar los responsables de las siguientes áreas:

a. Oficial de seguridad
b. Dueños de procesos.
c. Gerente del área.
d. Comité de seguridad.
e. Dueños de activos.
f. Coordinador del plan de contingencias.

El tratamiento de las vulnerabilidades identificadas, en la mayoría de los casos, implica su recuperación. Pero en función de los objetivos de negocio, de lo crítico de las mismas y del activo afectado, puede darse el caso que se acepte el riesgo asociado a una vulnerabilidad específica y ésta no se corrija. Un ejemplo de este caso son los sistemas obsoletos que todavía se encuentran en algunas organizaciones, los cuales pueden ser parte central de la operación del negocio de las mismas.

La recuperación en estos casos implica cambios profundos en los sistemas o bien el desarrollo de uno nuevo, con el riesgo que esto implica a la operación. En algunas ocasiones es posible implementar controles compensatorios que ayudan a reducir la exposición, minimizando el riesgo asociado a las vulnerabilidades identificadas.

Sin embargo, en la mayoría de los casos el proceso de recuperación implica la implementación de pequeños cambios al software, actualización o modificación de configuraciones.

2.6. Matriz de priorización de riesgos

2.6.1. Determinación del nivel de riesgo

La determinación del nivel de riesgo es el resultado de confrontar el impacto y la probabilidad con los controles existentes, al interior de los diferentes procesos y procedimientos que se realizan.

Para agilizar la determinación del nivel de riesgo se deben tener muy claros los puntos de control existentes en los diferentes procesos, los cuales permiten obtener información para efectos en la toma de decisiones.
Los niveles de riesgo pueden ser:

- *Zona de riesgo inaceptable*: Cuando el riesgo hace altamente vulnerable a la entidad o dependencia (impacto y probabilidad alta versus controles existentes).

- *Zona de riesgo importante o moderado*: Cuando el riesgo presenta una vulnerabilidad media (impacto alto - probabilidad baja o impacto bajo - probabilidad alta versus controles existentes).

- *Zona de riesgo aceptable*: Cuando el riesgo presenta vulnerabilidad baja (impacto y probabilidad baja versus controles existentes).

Lo anterior significa que a pesar de que la probabilidad y el impacto son altos, confrontado con los controles, se puede afirmar que el nivel de riesgo es medio, por lo tanto las acciones que se implementen entrarán a reforzar los controles existentes y a valorar la efectividad de los mismos.

2.6.2. Control de riesgo

Cualquier esfuerzo que emprenda la entidad en torno a la valoración de los riesgos llega a ser en vano, si no culmina en un adecuado manejo y control de los mismos definiendo acciones factibles y efectivas, tales como la implantación de políticas, estándares, procedimientos y cambios físicos entre otros, que hagan parte de un plan de manejo de riesgos.

Para el manejo del riesgo se pueden tener en cuenta alguna de las siguientes opciones, las cuales pueden considerarse cada una de ellas independientemente, interrelacionadas o en conjunto.

- *Evitar el riesgo*: Es siempre la primera alternativa por considerar. Se logra cuando al interior de los procesos se generan cambios sustanciales por mejoramiento, rediseño o eliminación, resultado de unos adecuados controles y acciones emprendidas. Un ejemplo de esto puede ser el control de calidad, manejo de los insumos, mantenimiento preventivo de los equipos, desarrollo tecnológico, etc.
- *Reducir el riesgo*: Si el riesgo no puede ser evitado porque crea grandes dificultades operacionales, el siguiente paso es reducirlo al más bajo nivel posible. La reducción del riesgo es probablemente el método más sencillo y económico para superar las debilidades antes de aplicar medidas más costosas y difíciles. Se consigue mediante la optimización de los procedimientos y la implementación de controles.
- *Dispersar y atomizar el riesgo*: Se logra mediante la distribución o localización del riesgo en diversos lugares; por ejemplo, la información de gran importancia se puede duplicar y almacenar en un lugar distante de ubicación segura, en vez de dejarla concentrada en un solo lugar, un ejemplo de ello es el procedimiento utilizado por la oficina de sistemas para salvaguardar la información que se genera diariamente en la entidad.

- Transferir el riesgo: Hace referencia a buscar respaldo y compartir con otro parte del riesgo; por ejemplo, tomar pólizas de seguros; se traslada el riesgo a otra parte o físicamente se traslada a otro lugar. Esta técnica es usada para eliminar el riesgo de un lugar y pasarlo a otro o de un grupo a otro.
- *Asumir el riesgo:* Luego que el riesgo ha sido reducido o transferido puede quedar un riesgo residual que se mantiene. En este caso, el gerente del proceso simplemente acepta la pérdida residual probable y elabora planes de contingencia para su manejo.

Una vez establecidas las opciones, es conveniente definir cuáles de las anteriores se van a concretar en la entidad, éstas deben evaluarse con relación al beneficio-costo para definir cuáles son susceptibles de ser aplicadas y proceder a elaborar el plan de su manejo.

2.6.3. Matriz de riesgos

2.6.3.1. Matriz para el análisis de riesgos

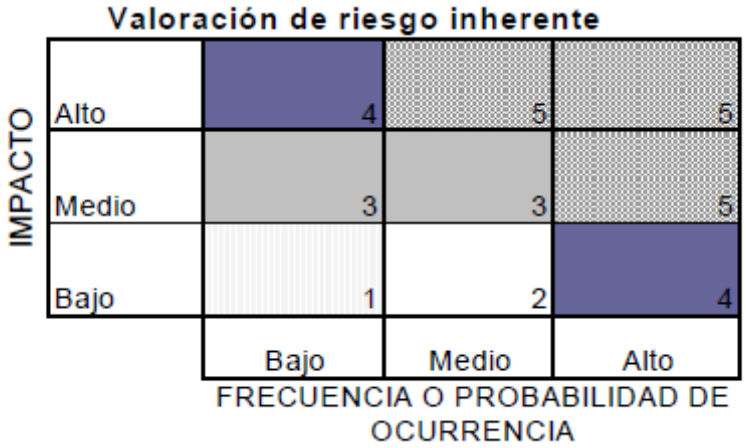
Una matriz de riesgos constituye una herramienta de control y de gestión, normalmente utilizada para identificar las actividades más importantes de una empresa, así como el tipo y nivel de riesgos inherentes a éstas y los factores externos e internos relacionados con los factores de riesgos. De igual forma una matriz de riesgos permite evaluar la efectividad de una adecuada gestión y administración de los riesgos financieros, que pudieran impactar los resultados y por lo tanto el logro de los objetivos de una organización.

La matriz de riesgos debe ser una herramienta flexible que documente los procesos y evalúe de manera integral el riesgo de una institución, a partir de los cuales se realiza un diagnóstico objetivo de la situación global de riesgo de un área. Una efectiva matriz de riesgo permite hacer comparaciones objetivas entre proyectos, áreas, productos, procesos o actividades. Todo ello constituye un soporte conceptual y funcional de un efectivo sistema integral de gestión de riesgo.

La valoración cualitativa no involucra la cuantificación de parámetros, utiliza escalas descriptivas para evaluar la probabilidad de ocurrencia de cada evento. En general este tipo de evaluación se utiliza cuando el riesgo detectado no justifica el tiempo y esfuerzo que requiera un análisis más profundo, o cuando no existe información suficiente para la cuantificación de los parámetros. En caso de que los riesgos afecten significativamente los resultados, la valoración cualitativa se utiliza como una evaluación inicial para identificar situaciones que ameriten un estudio más profundo.

Al respecto, debe notarse que si bien la valoración del riesgo contenida en una matriz de riesgos es mayormente de tipo cualitativo, también se utiliza un soporte cuantitativo basado en una estimación de eventos ocurridos en el pasado, con lo que se obtiene una mejor aproximación a la probabilidad de ocurrencia del evento.

La valoración consiste en asignar a los riesgos calificaciones dentro de un rango, que podría ser por ejemplo de 1 a 5 (insignificante (1), baja (2), media (3), moderada (4) o alta (5)), dependiendo de la combinación entre impacto y probabilidad. En la siguiente gráfica 2.1., se puede observar un ejemplo de esquema de valorización de riesgo en función de la probabilidad e impacto de tipo numérico con escala:



2.1. Valoración de riesgo.

Como se habrá podido observar la matriz de riesgo tiene un enfoque principalmente cualitativo, por lo que es preciso que quienes la construyan tengan experiencia, conocimiento profundo del negocio, su entorno y un buen criterio, pero además es requisito indispensable la participación activa de todas las áreas de la organización.

2.6.3.2. Tipos de matrices de riesgos

Mapa de riesgos

Conforme a la clasificación del riesgo por su impacto y frecuencia, se pueden graficar los éstos para identificar aquellos que son inherentes en una organización al usar Tecnologías de Información.

El mapa de riesgos 2.2. es uno de los medios que permite identificar factores de riesgos y cuantificación de frecuencias e impactos a través de un consenso de grupos de trabajo, entrevistas, cuestionarios y evaluaciones independientes, aprovechando la estadística disponible por incidencias o por lo contrario la experiencia de los responsables de cada área funcional, de apoyo y soporte. Se clasifican los riesgos de la organización determinando un punto de partida para desarrollar un marco completo para la administración del riesgo tecnológico. Cada cuadrante localizado en el mapa permite visualizar el nivel de exposición que se tiene por cada uno de los riesgos.

			Impacto				
			Menor	Bajo	Moderado	Alto	Critico
			1	2	3	4	5
Frecuencia	Esperado	5	Medio	Medio	Alto	Extremo	Extremo
	Muy Probable	4	Moderado	Medio	Medio	Alto	Extremo
	Probable	3	Moderado	Moderado	Medio	Alto	Alto
	Poco Probable	2	Bajo	Moderado	Medio	Medio	Alto
	Remoto	1	Bajo	Bajo	Moderado	Medio	Medio

2.2. Mapa de riesgos

El riesgo de acuerdo a su frecuencia e impacto se clasifica como:

Clasificación	Frecuencia	Descripción
5	Extremo	Indica que el riesgo tiene una gran probabilidad de ocurrencia y un impacto crítico para la organización en caso de materializarse.
4	Alto	Indica que el riesgo tiene una alta probabilidad de ocurrencia y un fuerte impacto para la organización en caso de materializarse.
3	Medio	Indica que el riesgo tiene una probabilidad de ocurrencia media e impacto significativo para la organización en caso de materializarse.
2	Moderado	Indica que el riesgo tiene cierta probabilidad de ocurrencia e impacto considerable para la organización en caso de materializarse.
1	Bajo	Indica que el riesgo tiene una mínima probabilidad de ocurrencia e impacto menor para la organización en caso de materializarse.

Al clasificar los riesgos a los que está expuesta la organización por frecuencia e impacto se tiene como resultado el mapa de riesgos con un listado de riesgos absolutos bajo un enfoque cualitativo.

2.6.4. El método RIIOT (Review, Interview, Inspect, Observe and Test) para la recolección de datos.

El método RIIOT es otra de las técnicas usadas en la evaluación de riesgos, en este caso para la fase de recolección de datos, la cual es el corazón del proceso de la evaluación de riesgos de seguridad; involucra volúmenes de datos, un enorme número de actividades y muchas horas de esfuerzo. La fase de recolección de datos es tal vez la fase de mayor labor de los procesos de evaluación de riesgos de seguridad y cubre todos los controles de seguridad de la organización, dentro de los límites del proyecto. A pesar de la complejidad de esta fase en la evaluación de los riesgos de seguridad de la información, pocas herramientas o métodos han sido desarrollados para que asistan en la planeación, desempeño y coordinación de estas actividades.

La revisión, entrevistas, inspección, observación y prueba del método RIIOT, aborda al problema de recolectar información en una amplia variedad de controles, usando un número grande de herramientas y técnicas. Algunas de las cuales se desarrollarán en el capítulo 5.

El método RIIOT considera cinco procesos para recolectar los datos, los cuales pueden ser aplicados a las áreas técnicas, administrativas y físicas de la organización, estos procesos son:

- *Revisar documentación.* Los miembros del equipo de evaluación de riesgos revisan la documentación que definen las reglas, configuraciones, planos, arquitecturas y otros elementos de control de seguridad. Todos los documentos disponibles y relevantes deben ser revisados, pueden incluir políticas, procedimientos, mapas de red, planos de centro de cómputos, bitácoras de respaldos y presentaciones de concientización de seguridad.
- *Entrevistas a personal clave.* Los miembros del equipo de evaluación de riesgos en sus entrevistas al personal clave, determinan la habilidad de dicho personal para realizar sus tareas –tal como debe estar definido en las políticas de la empresa evaluada-, su comportamiento en tareas no establecidas en dichas políticas y su manera de aplicarlas, así como las observaciones que tengan con los actuales controles de seguridad.
- *Inspección de controles de seguridad*. Los miembros del equipo de evaluación de riesgos inspeccionan los controles específicos de seguridad implementados, tales como el registro de visitantes, archivos de configuración, detectores de humo y el manejo de respuesta a incidentes. Estos controles pueden ser inspeccionados contra los estándares de la industria, con listados de verificación de puntos a revisar (checklists) de vulnerabilidades comunes o utilizando la experiencia y el juicio.

- *Observación del comportamiento del personal*. Los miembros del equipo de evaluación de riesgos observarán el comportamiento del personal, la capacidad del cuerpo de seguridad y otros, durante el curso de la evaluación. Estas observaciones pueden proveer una visión precisa de la efectividad de los controles de seguridad en el lugar.
- *Pruebas de controles de seguridad.* Los miembros del equipo de evaluación de riesgos probarán controles de seguridad específicos, tales como firewalls, servidores, alarmas al abrir puertas y sensores de movimiento. Casi todos los métodos de evaluación de riesgos de seguridad apuntan a la revisión de estos controles. Las pruebas involucran el uso de escáneres de vulnerabilidad para los controles de seguridad lógicos, además de métodos específicos para controles físicos, tales como el intercambio de sensores de movimiento.

Estos puntos de vista serán utilizados y descritos con más detenimiento en el capítulo 5.

CAPÍTULO 3

METODOLOGÍAS DE EVALUACIÓN DE RIESGOS EN TECNOLOGÍAS DE INFORMACIÓN

CAPÍTULO 3

METODOLOGÍAS DE EVALUACIÓN DE RIESGOS EN TECNOLOGÍAS DE INFORMACIÓN

3.1. Introducción

La Informática ha sido tradicionalmente una materia compleja en todos sus aspectos, por lo que se hace necesaria la utilización de metodologías en cada doctrina que la componen, desde su diseño de ingeniería hasta la auditoría de los sistemas de información.
Las metodologías usadas por un profesional dicen mucho de su forma de entender su trabajo y están directamente relacionadas con su experiencia profesional, acumulada como parte del comportamiento humano de "prueba y error".

La *evaluación de riesgos en tecnologías de información* es el proceso de comparar el nivel de riesgo encontrado durante el análisis de los mismos, contra el criterio de riesgo establecido previamente y decidir el tratamiento que se dará a éstos.

El análisis de riesgos y los criterios contra los cuales éstos son comparados en la valoración, deben ser considerados sobre la misma base. Así, evaluaciones cualitativas incluyen la comparación de un nivel cualitativo de riesgo contra criterios cualitativos y evaluaciones cuantitativas involucran la comparación de niveles estimados de riesgo contra criterios que pueden ser expresados con números específicos, tales como fatalidad, frecuencia o valores monetarios.

El resultado de una evaluación de riesgos para cualquier criterio, es una lista priorizada de riesgos para definir posteriormente acciones de tratamiento a cada uno de ellos.

3.2. Metodologías de análisis de riesgos

Todas las metodologías existentes desarrolladas y utilizadas en el análisis y evaluación de riesgos en Tecnologías de Información, se pueden agrupar en dos grandes familias.

- *Cuantitativas*: Basadas en un modelo matemático que ayuda a la realización del trabajo.
- *Cualitativas:* Basadas en el criterio y raciocinio humano, capaz de definir un proceso de trabajo para seleccionar, con base en la experiencia acumulada.

Estas metodologías están desarrolladas para la identificación de la falta de controles y el establecimiento de un plan para minimizar o eliminar las causas principales del riesgo.

3.2.1. Metodologías cuantitativas

Este tipo de metodologías han sido diseñadas para producir una lista de riesgos que son comparables entre sí, para facilitar el poder asignarles valores numéricos. Estos valores en el caso de metodologías de análisis de riesgos son datos de probabilidad de ocurrencia de una situación o evento, que se deben extraer de un registro de incidencias, donde el número de incidencias sea suficientemente grande o tienda al infinito. Esto no se aplica con precisión en la práctica, ya que lo común es que se aproxime ese valor de forma subjetiva restando así rigor científico al cálculo. Siendo que el cálculo se hace para ayudar a elegir el método entre varias respuestas al riesgo, esta aproximación podría ser aceptada.

Hay varios coeficientes que conviene definir para esta metodología:

- *Expectativa de pérdida por evento (SLE):* la expectativa de pérdida por evento, es la pérdida esperada como el resultado de un solo evento. En algunas técnicas de evaluación de riesgos de seguridad es usada una fórmula específica para el SLE, que incorpora un factor de exposición (EF), y el valor del activo (VA). Se define el factor de exposición, como el valor de pérdida promedio del activo por evento. Por ejemplo, en el caso de un incendio de un centro de datos, suponiendo que solo se queme la mitad, o visto de otra manera, se pierda sólo la mitad de su valor; esto resulta en un factor de exposición de 0.50. Añadiendo este factor, se tiene que la expectativa de pérdida por evento, se define como el valor del activo multiplicado por el factor de exposición.

(SLE) = (AV) x (EF).

- *ALE (Annualized Loss Expectacy*): es inusual que un evento de riesgo en la seguridad ocurra solamente una vez al año. Tal vez el riesgo de que un centro de datos se incendie, puede ocurrir una vez cada veinte años; sin embargo, los eventos de riesgos de seguridad como los virus informáticos suceden frecuentemente durante un año. Pero como los presupuestos para evitar o reducir estos incidentes sólo se realizan una vez al año, de aquí la utilidad de calcular las pérdidas esperadas por la ocurrencia de estos eventos durante un año. A este número se le conoce como la expectativa de pérdida anualizada (ALE). Este coeficiente se obtiene de multiplicar la expectativa de pérdida por evento, por el índice anual de ocurrencia (ARO).Para el cálculo de este coeficiente, el ARO es simplemente una predicción de la frecuencia, con la que un evento de riesgo en la seguridad puede ocurrir cada año. Un ejemplo, es el índice anual de ocurrencia de seis eventos al año ó 6/1 ó 6, de posibles ataques de virus informáticos, mientras que el índice de ocurrencia de un incendio en un centro de datos puede ser de 1/20 ó 0.005.

ALE= SLE x ARO

- *Valor del costo de prevención de un riego*: por último, es de gran utilidad el determinar cuánto estamos dispuestos a invertir en una medida de prevención, para reducir un riesgo de seguridad específico. Definiendo como medida de prevención a cualquier mecanismo de seguridad técnico, administrativo o físico, que reduzca el riesgo de seguridad a los activos de la organización. Estas medidas cuestan tiempo y dinero para implementarse, ya que no garantizan la eliminación total del riesgo, por lo que la evaluación del costo de implementación contra la pérdida del activo es lo que definirá la ejecución de dichas medidas. Si la reducción del riesgo de seguridad a los activos de la empresa no es significativo y el costo de las medidas para reducir dicho riesgo es alto, pudiera desecharse dicha medida. Finalmente, podemos definir el valor del costo de prevención de un riesgo, como la reducción apreciada en la expectativa de pérdida esperada menos el costo anual de implementar una medida de prevención.

Estos coeficientes y algunos otros son utilizados para la simulación que permite elegir entre varias contramedidas en el análisis de riesgos.

Ventajas de las metodologías cuantitativas:

- *Objetividad*: Una variable de decisión de riesgo de seguridad determinada a través del análisis cuantitativo pueden ser considerada como objetiva, ya que los cálculos que determinan los valores de las variables son basados en fórmulas predeterminadas y no son influenciadas por medidas subjetivas o por el juicio del equipo.
- *Expresiones en números "reales":* La evaluación de los activos y la valoración del costo de protección de dichos activos, pueden ser siempre expresados en términos de costos específicos (monetarios).

Sus desventajas son:

- *Complejidad*: Las fórmulas usadas en este tipo de análisis y el volumen de tablas numéricas resultantes pueden ser muy complejas. Esto lleva entre otros problemas a la necesidad de personas más experimentadas dentro del equipo de evaluación, lo que conlleva a un incremento en el costo total.
- *Cálculos no entendidos*: Los cálculos y resultados pueden ser una amenaza para el lector no técnico, como el staff de dirección; por lo que puede malinterpretarse el análisis efectuado y sus resultados.
- *Resultados no confiables*. Las fórmulas complejas y la falta de entendimiento de los cálculos pueden llevar a una frustración general e inclusive a la desconfianza en los resultados. No es fácil aceptar las recomendaciones finales cuando no se entiende el análisis.

- *Trabajo excesivo:* Un análisis de riesgos de seguridad de la información puede ser muy demandante en cuanto a la cantidad de trabajo, por el número de datos requeridos y los cálculos que necesitan ser realizados. Se requiere la recolección de una gran cantidad de datos para obtener los valores necesarios y así poder aplicar las fórmulas cuantitativas. La determinación de un valor para los activos, amenazas, vulnerabilidades y el costo de protección de los activos ya es suficientemente difícil, como para agregar a ello, la necesidad de un acuerdo entre los miembros del equipo para cada uno de los valores involucrados.
- *Falso sentido de precisión.* Tal vez la mayor desventaja de los métodos de evaluación de riesgos cuantitativos es el falso sentido de precisión que se refleja en la mayoría de los consumidores de esta información. Cuando se entrega un reporte de evaluación de riesgos en TI, con números y cifras específicas de pérdidas esperadas o valores de costos de protección de los activos, los consumidores tienden a creer que las cifras son generadas con un alto nivel de precisión. El hecho es que es muy difícil calcular un valor preciso para las múltiples variables involucradas, por lo que este valor esta típicamente basado en elementos subjetivos tales como la opinión, por lo que la precisión presentada no es siempre acertada.

3.2.2. Metodologías cualitativas

Precisan de la participación de un profesional experimentado. Estas metodologías están basadas en métodos estadísticos y lógica difusa (humana, no matemática); pero requieren menos horas/hombre que las metodologías cuantitativas.
Los mismos elementos básicos que son requeridos para determinar la seguridad del riesgo, tales como los valores del activo, la frecuencia del riesgo, el impacto y la efectividad de protección al activo bajo el punto de vista cuantitativo, también son usados bajo las metodologías cualitativas, sólo que ahora son medidos en términos subjetivos, tales como “alto o poco probable”.

- Ventajas de las metodologías cualitativas sobre el punto de vista cuantitativo:

  - *Simple*: Estos métodos son un alivio a la complejidad de los modelos cuantitativos. La simplicidad de estos métodos son la característica principal y a su vez la raíz de casi todas sus desventajas.
  - *Valores de medida simples:* El utilizar métodos cuantitativos puede ser extremadamente difícil de proveer números precisos para cada una de las variables, como son los activos, amenazas, impactos o valores de protección del activo. Usando métodos cualitativos, esta tarea es aún significativa, pero puede ser realizada usando un esfuerzo mayor.
  - *Fácil de entender y convenir*: El análisis y resultado de los métodos cualitativos son fáciles de ser aceptados y acordados por el equipo.

- *Identificación adecuada de las áreas con problemas:* En la mayoría de las situaciones, un punto de vista cualitativo nos dará suficiente información para influenciar una mejor postura de la organización en cuanto a la seguridad.

- Desventajas de las metodologías cualitativas:

  - *Resultados* subjetivos: Ya que los resultados son basados principalmente en la experiencia y juicio, más que en números, porcentajes o cifras; éstos pueden ser argumentados como poco precisos.
  - *Valor de activos subjetivos:* El mismo argumento arriba mencionado, es usado para la valoración subjetiva de los activos. Es difícil defender valores subjetivos asignados a los activos, cuando se basan únicamente en la experiencia.
  - *Recomendaciones subjetivas*: Si el análisis es basado en valores y resultados subjetivos, entonces las recomendaciones resultantes son también subjetivas.
  - *Dificultad para rastrear las mejoras:* En los programas de seguridad que buscan dar seguimiento entre evaluaciones, se vuelve difícil rastrear el avance cuando los resultados de éstas son definidas como riesgo de seguridad “alto-medio” o “medio-bajo”.

3.3. Metodologías de auditoría informática

Las únicas metodologías que podemos encontrar en la auditoría informática son dos familias distintas: las auditorías de controles generales y las metodologías de los auditores internos.

- *Metodologías de auditorías de controles generales:* El objetivo de las auditorías de controles generales consiste en dar una opinión sobre la fiabilidad de los resultados para la auditoría financiera. El resultado es un breve informe como parte de la documentación de la auditoría, donde se destacan las vulnerabilidades encontradas. Estás metodologías están basadas en pequeños cuestionarios estándares que dan como resultado informes muy generales.

- *Metodologías de los auditores internos:* Están formadas por recomendaciones que integran parte del plan de trabajo y además se deben crear metodologías propias necesarias para auditar áreas o aspectos que definan el plan auditor.

Las metodologías de auditoría son del tipo cualitativo. Se puede decir que son subjetivas por excelencia. Por lo tanto, están sustentadas en profesionales de gran nivel de experiencia y formación, capaces de dar recomendaciones técnicas, operativas y jurídicas, que exigen una gran profesionalidad y formación continua.

Entre las dos metodologías de evaluación de sistemas (análisis de riesgos y auditoría informática) existen similitudes y grandes diferencias. Ambas tienen documentación obtenida del trabajo de campo tras el plan de entrevistas, pero los cuestionarios son totalmente distintos.

3.4. Metodologías de clasificación de la información y de la obtención de los procedimientos de control.

3.4.1. Metodologías de clasificación de la información

Encontrar metodologías de este tipo no es frecuente, pero la metodología PRIMA (Prevención de riesgos informáticos con metodología abierta) desarrolla específicamente estos dos aspectos, mismos que se muestran a continuación.

- *Clasificación de información*: el análisis de riesgos metodológicamente permite clasificar una variedad de contramedidas de acuerdo a la probabilidad del riesgo analizado, siendo que todas las entidades de información a proteger no tienen el mismo grado de importancia.
- *Obtención de los procedimientos de control*: cuyo objetivo es optimizar la eficiencia de los procedimientos de control y reducir los costos de los mismos, de acuerdo a las contramedidas para las distintas áreas con diferente nivel de vulnerabilidad.

Esta metodología PRIMA es del tipo cualitativo y como el resto de la misma, tiene listas de ayuda, por lo que el profesional puede añadir en la herramienta que seleccione: niveles o jerarquías, estándares y objetivos a cumplir por nivel.

3.4.2. Metodología de la obtención de los procedimientos de control

En la metodología de la obtención de los procedimientos de control, es frecuente encontrar manuales de operación de todas las áreas de la empresa, que explican las funciones y cómo se realizan las distintas tareas diariamente, siendo éstos necesarios para que los profesionales puedan realizar las revisiones operativas, evaluando si los procedimientos son correctos, están aprobados, y sobre todo si se cumplen.

Los procedimientos efectuados para asegurar el cumplimiento de los objetivos son definidos como controles. El cumplimiento de las metas indica claramente que estos procedimientos tienen un efecto directo y mitigante sobre los riesgos existentes.

A continuación se definen las diferentes tareas que pueden contribuir con los proyectos de un plan de seguridad, a fin de mejorar las contramedidas ya establecidas:

Fase I. Definición de objetivos de control.

Tarea 1: Análisis de la empresa. Se estudian los organigramas, funciones y procesos.

Tarea 2: Recopilación de estándares. Se estudian todas las fuentes de información necesarias, para lograr definir en la siguiente fase los objetivos de control por cumplir (por ejemplo: ISO, CISA, etc.).

Tarea 3: Definir los objetivos de control.

Fase II. Definición de los controles.

Tarea 1: Definir los controles. Con los objetivos de control definidos, se analizan los procesos y se van definiendo los distintos controles que se requieran.

Tarea 2: Definición de necesidades tecnológicas (hardware y herramientas de control).

Tarea 3: Definición de los procedimientos de control. Se desarrollan los distintos procedimientos que se generan en las áreas de: usuarios, informática y control informático, entre otros.

Tarea 4: Definición de las necesidades de recursos humanos.

Fase III. Implantación de los controles.

Una vez definidos los controles, las herramientas de control y los recursos humanos necesarios, se procede a implantarlos en forma de acciones específicas.

Terminado el proceso de implantación de acciones habrá que documentar los procedimientos nuevos y revisar los cambios efectuados. Los procedimientos resultantes serán:

- Procedimientos propios de control de la actividad informática (control interno informático).
- Procedimientos de distintas áreas de usuarios de la informática.
- Procedimientos de áreas informáticas.
- Procedimientos de control que relacionan las diferentes áreas de informática, control interno informático y el área informática, los usuarios informáticos y el área de control no informático.

3.5. Otras metodologías de evaluación de riesgos

Todas las metodologías de evaluación de riesgos en Tecnologías de Información tienen los mismos elementos básicos los cuales son:

- El análisis de riesgo.
- La valoración de activos.
- Análisis de vulnerabilidad.
- Evaluación de riesgos de seguridad.

Una metodología de evaluación de riesgos en Tecnologías de Información puede ser ideal para una organización, pero no para otras con diferentes circunstancias. Debido a las distintas necesidades, se han desarrollado una variedad de metodologías de evaluación de riesgos en TI.

3.5.1. Proceso de gestión de riesgos de seguridad de la Administración Federal de Aviación (Federal Aviation Administration ,FAA)

La gestión de procesos de riesgos de seguridad (Security Risk Management, SRM) fue desarrollada por la FAA para lograr el objetivo de gestionar los riesgos de seguridad en todo el proceso de administración de sus actividades.

Esta gestión de procesos también es aplicable a otras organizaciones y consiste de un método cualitativo que proporciona niveles, descripciones y fórmulas para los cálculos respectivos; sin embargo, no ofrece mucho en cuanto a ejemplos, plantillas, listas de comprobación o herramientas.

3.5.2. Metodología OCTAVE

Esta metodología de evaluación de riesgos de seguridad fue desarrollada por el Instituto de Ingeniería de la Universidad de Carnegie Mellon Software.

El método de evaluación de vulnerabilidades, activos y amenazas críticas operacionales (Operationally Critical Threat, Asset, and Vulnerability Evaluation, OCTAVE) ofrece un proceso completo con las normas, listas de control, estimaciones de tiempo y describe el proceso de evaluación de riesgos de seguridad en tres fases, las cuales son:

- Perfiles de amenazas basados en los activos.
- La identificación de vulnerabilidades en la infraestructura.
- El desarrollo del plan de seguridad.

Este método esta diseñado para ser implementado por un equipo pequeño, dentro de una organización grande (300 ó más personas) con una jerarquía de múltiples áreas, una infraestructura informática establecida internamente y con la posibilidad de ejecutar sus propias herramientas de evaluación de vulnerabilidad. El equipo puede tener algún tipo de capacitación y experiencia al realizar una evaluación, lo que no supone que sean expertos.

3.5.3. Proceso de evaluación FRAP

El proceso de evaluación de riesgos facilitado (Facilitated Risk Assessment Process, FRAP) fue desarrollado por Tom Peltier en 2001 y diseñado como una metodología que podría ser utilizada por los propios directivos, con la guía de un profesional capacitado.

El método FRAP consiste de tres pasos, los cuales están diseñados para ser completados en 10 días. Éste es un método cualitativo, que se auxilia de plantillas y listas de verificación (checklist).

3.5.4. Método de gestión y análisis de riesgos CRAMM

El método de gestión y análisis de riesgos (Risk Analysis and Management Method, CRAMM) de la Agencia Central de Informática y Telecomunicaciones del Gobierno Británico (Central Computer and Telecommunications Agency, CCTA), fue desarrollado por el gobierno británico en 1985. Hoy en día este método ha evolucionado y es comercializado por Insight Consulting.

CRAMM es una herramienta cualitativa que proporciona: una metodología, los cálculos a realizarse y el formato de reporte para una evaluación de riesgos de seguridad.

3.5.5. NSA IAM

La metodología de evaluación InfoSec (InfoSec Assessment Methodology,IAM) de la agencia de Seguridad Nacional (National Security Agency's, NSA) fue desarrollada para capacitar a las entidades comerciales, en la realización de las evaluaciones de los estándares de la NSA. Esta metodología se basa en el enfoque de la agencia, para la evaluación de seguridad de la información en entidades gubernamentales.

La evaluación de esta metodología consiste en tres fases:

- Pre-evaluación.
- La visita en sitio.
- Y la post-evaluación.

La documentación de la metodología proporciona plantillas y guías para cada paso del proceso, incluyendo una lista de 18 actividades base principales.

El proceso de evaluación aproximadamente tarda de cinco a catorce semanas para ser completado y se recomienda un equipo de dos o tres personas para realizarlo.

CAPÍTULO 4

TRATAMIENTO DE RIESGOS EN TECNOLOGÍAS DE INFORMACIÓN

CAPÍTULO 4

TRATAMIENTO DE RIESGOS EN TECNOLOGÍAS DE INFORMACIÓN

4.1. Normas y estándares internacionales

Dados los continuos cambios en las Tecnologías de Información, en este capítulo se menciona el tratamiento de riesgos y algunas normativas que se han desarrollado conforme han ido evolucionado éstas.

Estas normativas constituyen el fundamento para el avance en el desarrollo de los controles en las áreas de TI, gestionando la seguridad de la información utilizable en cualquier tipo de organización, ya sea pública o privada, grande o pequeña.

Las organizaciones necesitan un conjunto estructurado, sistemático, coherente y completo de normas a seguir, a fin de identificar los riesgos a los que están sometidas para así tomar medidas adecuadas y proporcionadas de una correcta gestión de seguridad.

4.1.1. COBIT

COBIT (Control OBjectives for Information and related Technology | Objetivos de Control para tecnología de la información y relacionada) es el modelo para el gobierno de las Tecnologías de Información, desarrollado por la Asociación de Auditoría y Control de Sistemas de Información (Information Systems Audit and Control Association, ISACA) y el Instituto de Gobierno de TI (IT Governance Institute, ITGI). La última versión de este modelo es la 5.0.

COBIT4 tiene 34 objetivos a nivel alto, que cubren 215 objetivos de control clasificados en los siguientes cuatro dominios:

- Planear y Organizar
- Adquirir e Implementar
- Entregar y Dar Soporte
- Monitorear y Evaluar

COBIT4 tiene 34 objetivos a nivel alto, que cubren 215 objetivos de control clasificados en cuatro dominios, éstos, con sus objetivos de alto nivel se muestran a continuación:

- **Planear y Organizar**

  - PO1 Definir un plan estratégico de TI
  - PO2 Definir la arquitectura de la Información
  - PO3 Determinar la dirección tecnológica
  - PO4 Definir los procesos, organización y relaciones de TI
  - PO5 Administrar la inversión en TI
  - PO6 Comunicar las aspiraciones y la dirección de la gerencia
  - PO7 Administrar recursos humanos de TI
  - PO8 Administrar la calidad
  - PO9 Evaluar y administrar los riesgos de TI
  - PO10 Administrar proyectos

- **Adquirir e Implementar**

  - AI1 Identificar soluciones automatizadas
  - AI2 Adquirir y mantener software aplicativo
  - AI3 Adquirir y mantener infraestructura tecnológica
  - AI4 Facilitar la operación y el uso
  - AI5 Adquirir recursos de las TI
  - AI6 Administrar cambios
  - AI7 Instalar y acreditar soluciones y cambios

- **Entregar y Dar Soporte**

  - DS1 Definir y administrar los niveles de servicio
  - DS2 Administrar los servicios de terceros
  - DS3 Administrar el desempeño y la capacidad
  - DS4 Garantizar la continuidad del servicio
  - DS5 Garantizar la seguridad de los sistemas
  - DS6 Identificar y asignar costos
  - DS7 Educar y entrenar a los usuarios
  - DS8 Administrar la mesa de servicio y los incidentes
  - DS9 Administrar la configuración
  - DS10 Administrar los problemas
  - DS11 Administrar los datos
  - DS12 Administrar el ambiente físico
  - DS13 Administrar las operaciones

- **Monitorear y Evaluar**

  - ME1 Monitorear y evaluar el desempeño de TI
  - ME2 Monitorear y evaluar el control interno
  - ME3 Garantizar el cumplimiento regulatorio
  - ME4 Proporcionar gobierno de TI

Independientemente de la situación tecnológica en cada escenario u organización, COBIT5 determina un conjunto de mejores prácticas para obtener una mayor calidad y eficiencia en seguridad, siendo necesarias estas prácticas para: identificar riesgos, entregar valor al negocio, gestionar y medir el desempeño de los recursos, el cumplimiento de metas y el nivel de madurez de los procesos de la organización.

COBIT5, actualmente en su versión 5.0, está basado en cinco principios clave para la gobernabilidad y manejo de las TI en la organización:

- *Principio 1. Satisfacer las necesidades de las partes interesadas:* Las empresas existen para crear valor para sus partes interesadas manteniendo el equilibrio entre la generación de beneficios y la optimización de los riesgos y el uso de recursos. COBIT5 provee todos los procesos necesarios y otros facilitadores para permitir la creación de valor del negocio mediante el uso de las TI. Dado que toda empresa tiene objetivos diferentes, una empresa puede personalizar COBIT5 para adaptarlo a su propio contexto mediante la cascada de metas, traduciendo metas corporativas de alto nivel en otras metas más manejables, específicas, relacionadas con TI, mapeándolas con procesos y prácticas específicos.
- *Principio 2. Cubrir la empresa extremo-a-extremo:* COBIT5 integra el gobierno y la gestión de TI en el gobierno corporativo.
  - Cubre todas las funciones y procesos dentro de la empresa; COBIT 5 no se enfoca sólo en la "función de TI", sino que trata la información y las tecnologías relacionadas como activos que deben ser tratados como cualquier otro activo por todos los miembros de la empresa.
  - Considera que los facilitadores relacionados con TI para el gobierno y la gestión, deben ser a nivel de toda la empresa y de principio a fin, es decir, incluyendo a todo y todos –internos y externos– los que sean relevantes para el gobierno y la gestión de la información de la empresa.

- *Principio 3. Aplicar un marco de referencia único integrado*: Hay muchos estándares y buenas prácticas relativos a TI, ofreciendo cada uno ayuda para un subgrupo de actividades de éstas. COBIT5 se alinea a alto nivel con otros estándares y marcos de trabajo relevantes, de este modo puede hacer la función de marco de trabajo principal para el gobierno y la gestión de las TI de la empresa.

- *Principio 4. Hacer posible un enfoque holístico*: Un gobierno y gestión de las TI de la empresa eficiente y eficaz, requiere de un enfoque holístico que tenga en cuenta varios componentes interactivos. COBIT5 define un conjunto de facilitadores (*enablers*) para apoyar la implementación de un sistema de gobierno y gestión global para las TI de la empresa. Los facilitadores se definen a grandes rasgos como cualquier cosa que puede ayudar a conseguir las metas de la empresa. El marco de trabajo de COBIT5 define siete categorías de facilitadores:
  - Principios, políticas y marcos de trabajo
  - Procesos
  - Estructuras organizativas
  - Cultura, ética y comportamiento
  - Información
  - Servicios, infraestructuras y aplicaciones
  - Personas, habilidades y competencias

- *Principio 5. Separar el gobierno de la gestión*: El marco de trabajo de COBIT5 establece una clara distinción entre gobierno y gestión. Estas dos disciplinas engloban diferentes tipos de actividades, requieren distintas estructuras organizativas y sirven a diferentes propósitos. La visión de COBIT5, en esta distinción clave, entre gobierno y gestión es:
  - *Gobierno:* El Gobierno asegura que se evalúan las necesidades, condiciones y opciones de las partes interesadas para determinar que se alcanzan las metas corporativas equilibradas y acordadas; estableciendo la dirección a través de la priorización y la toma de decisiones; midiendo el rendimiento, el cumplimiento respecto a la dirección y metas acordadas.
    En muchas corporaciones, el gobierno global es responsabilidad del comité de dirección bajo el liderazgo del presidente. Algunas responsabilidades de gobierno específicas se pueden delegar en estructuras organizativas especiales al nivel apropiado, particularmente en las corporaciones más grandes y complejas.
  - *Gestión:* La gestión planifica, construye, ejecuta y controla actividades alineadas con la dirección establecida por el cuerpo de gobierno para alcanzar las metas empresariales.
    En muchas empresas, la gestión es responsabilidad de la dirección ejecutiva bajo el liderazgo del Director General Ejecutivo (CEO).

Juntos, estos cinco principios habilitan a la empresa a construir un marco de gestión de gobierno y gestión efectiva que optimiza; la inversión y el uso de información y tecnología para el beneficio de las partes interesadas.

La familia de productos COBIT5 es:

- COBIT5 Habilitando procesos
- COBIT5 Implementación
- COBIT5 Seguridad de la información
- COBIT5 Certificación (Assurance)
- COBIT5 Programa de evaluación
- COBIT5 Riesgo

El riesgo es definido, generalmente, como la combinación de la probabilidad de un evento y su consecuencia. COBIT5 Riesgo, define el riesgo en TI como un riesgo del negocio, específicamente asociado con el uso, propiedad, operación, involucramiento, influencia y adopción dentro de la empresa.

COBIT5 Riesgo provee:

- Las partes interesadas con una mejor comprensión de los efectos del estado y el riesgo actual en toda la empresa
- Orientación sobre cómo manejar el riesgo a niveles, que incluye un amplio conjunto de medidas
- Orientación sobre cómo configurar la cultura del riesgo adecuada para la empresa
- Orientación sobre las evaluaciones de riesgos que permiten a las partes interesadas a considerar el costo de la mitigación y los recursos necesarios contra la exposición a las pérdidas
- Oportunidades para integrar la gestión de riesgos con el riesgo de la empresa
- Mejora de la comunicación y el entendimiento entre todos los grupos de interés internos y externos

4.1.2. ISO 27000

La información (datos) dentro y fuera de una organización, es un activo vital para la superación y continuidad de cualquier organización en el mercado. Con objeto de una adecuada gestión de la seguridad de la información, es necesario implementar un sistema que aborde esta tarea en forma metódica, documentada y basada en objetivos claros de seguridad.

ISO/IEC 27000. Conjunto de estándares desarrollados por la Organización Internacional de Estandarización (International Organization for Standardization, ISO) y la Comisión Electrotécnica Internacional (International Electrotechnical Commission, IEC), que proporcionan un marco de gestión de seguridad de la información para cualquier tipo de organización, pública o privada, ya sea grande o pequeña.

- *ISO/IEC 27000. P*ublicada el 1° de mayo de 2009 y revisada como una segunda edición el 1° de diciembre de 2012. Esta norma proporciona una visión general de las normas que componen la serie 27000, así como una introducción a los Sistemas de Gestión de Seguridad de la Información y una breve descripción de términos y definiciones que se emplean en toda esta serie 27000.

Esta familia de normas tiene como objetivo definir requerimientos para un sistema de gestión de la seguridad de la información (SGSI), con el fin de garantizar la selección de controles de seguridad adecuados, protegiendo así la información, es recomendable para cualquier empresa, más especialmente para aquellos sectores que tengan información crítica o gestionen la información de otras empresas; a continuación se mencionan algunas normas.

- *ISO/IEC 27001*. Publicada el 15 de octubre de 2005. Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información (SGSI). Tiene su origen en la BS 7799-2:2002 (que ya quedó anulada) y es la norma con arreglo a la cual se certifican por auditores externos los SGSI de las organizaciones. Enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005, para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI. Actualmente, este estándar se encuentra en periodo de revisión en el subcomité ISO SC27, con fecha prevista de publicación para 2014.
- *ISO/IEC 27002*. Desde el 1 de julio de 2007 es el nuevo nombre de ISO 17799:2005, siendo 2005 el año de edición. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios. Actualmente, este estándar se encuentra en periodo de revisión en el subcomité ISO SC27, con fecha prevista de publicación de la segunda edición en mayo de 2014.
- *ISO/IEC 27003*. Publicada el 1° de febrero de 2010. Es una guía que se centra en los aspectos críticos necesarios para el diseño e implementación con éxito de un SGSI de acuerdo con ISO/IEC 27001:2005. No certificable.
- *ISO/IEC 27004*. Publicada el 15 de diciembre de 2009. Es una guía para el desarrollo y utilización de métricas y técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles o grupos de controles implementados según ISO/IEC 27001. No certificable.

- *ISO/IEC 27005*. Publicada la 2ª edición el 1° de junio de 2011 (1primera edición del 15 de Junio de 2008). Proporciona directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos. No certificable.
- *ISO/IEC 27006*. Publicada en 2ª edición el 1 de Diciembre de 2011 (1ª edición del 1 de marzo de 2007). Especifica los requisitos para la acreditación de entidades de auditoría y certificación de SGSI.
- *ISO/IEC 27007*. Publicada el 14 de noviembre de 2011. Es una guía de auditoría de un SGSI, como complemento a lo especificado en ISO 19011. No certificable.
- *ISO/IEC TR 27008*. Publicada el 15 de octubre de 2011. Es una guía de auditoría de los controles seleccionados en el marco de implantación de un SGSI. No certificable.
- *ISO/IEC 27010*. Publicada el 20 de octubre de 2012. Consiste en una guía para la gestión de la seguridad de la información cuando se comparte entre organizaciones o sectores. Es aplicable a todas las formas de intercambio y difusión de información sensible, en organizaciones tanto públicas como privadas, a nivel nacional e internacional, dentro de la misma industria o sector de mercado o entre sectores.
- *ISO/IEC 27011.* Publicada el 15 de diciembre de 2008. Es una guía de interpretación de la implementación y gestión de la seguridad de la información en organizaciones del sector de telecomunicaciones *basada en ISO/IEC 27002.*
- *ISO/IEC 27013*. Publicada el 15 de octubre de 2012. Es una guía de implementación integrada de ISO/IEC 27001 (gestión de seguridad de la información) y de ISO/IEC 20000-1 (gestión de servicios de TI).
- *ISO/IEC 27014.* En fase de desarrollo, con publicación prevista en 2013. Consistirá en una guía de gobierno corporativo de la seguridad de la información.
- *ISO/IEC TR 27015.* Publicada el 23 de noviembre de 2012. Es una guía de SGSI orientada a organizaciones del sector financiero y de seguros y como complemento a ISO/IEC 27002.

4.2. Revisión de controles de seguridad existentes

Los controles son las medidas utilizadas para prevenir o reducir el impacto de eventos no deseados. Los métodos de control pueden ser:

- Controles físicos (hardware, software).
- Controles lógicos o técnicos (políticas de seguridad, procedimientos administrativos y operacionales, seguridad física).
- Controles administrativos.

Los controles por su naturaleza pueden clasificarse como:

Preventivos. Son los que actúan sobre la causa de los riesgos con el fin de disminuir su probabilidad de ocurrencia y constituyen la primera línea de defensa. También actúan para reducir la acción de los agentes generadores de riesgos

*Detectivos. S*on los que se diseñan para descubrir un evento, irregularidad o resultado no previsto. Alertan sobre la presencia de riesgos y permiten tomar medidas inmediatas.

Correctivos. Son los que permiten el restablecimiento de la actividad después de ser detectado el evento no deseable y la modificación de las acciones que propiciaron su ocurrencia.

Manuales. Son los ejecutados por personas.

Automatizados. Son los ejecutados por sistemas de información.

Para que los controles sean efectivos, éstos deben estar integrados en lo que se denomina una arquitectura de seguridad informática, la cual proporciona una visión sistémica de la infraestructura y administración de la seguridad informática dentro de la empresa, además de ser congruente con los objetivos de la organización y las prioridades de las posibles amenazas de acuerdo al impacto que éstas tengan en la empresa.

Por lo tanto, una fase fundamental en el diseño de la arquitectura de seguridad informática, es la etapa de análisis de riesgos.

Los controles deben ser capaces, eficaces y oportunos, para esto es preciso conocer el entorno de los riesgos y su frecuencia, así como las consecuencias que implican, para que las actividades y los procesos mantengan el rumbo de las normas establecidas.

Para los controles aplicables se hace una ponderación con el fin de determinar qué tan eficaces y maduros son los controles establecidos para mitigar los riesgos identificados; conforme a lo indicado en la tabla 4.1..

Ponderación	Descripción
5	Los procedimientos y medidas de control están formalizados y siempre son utilizados, aplicados, medidos y monitoreados. Además de ser optimizados periódicamente.
4	Los procedimientos y medidas de control están formalizados y siempre son utilizados, aplicados, medidos y monitoreados.
3	Los procedimientos y medidas de control están formalizados y siempre son utilizados y aplicados.
2	Los procedimientos o medidas de control no están formalizados y no siempre son utilizados o aplicados.
1	Se tiene conciencia sobre la necesidad de contar con procedimientos o medidas de control.
0	No se cuenta con políticas o procedimientos.

Tabla 4.1. Ponderación de controles.

4.3. Políticas y procedimientos

Como ya se ha mencionado, la administración de riesgos recae sobre la dirección del área y sobre los gerentes de la misma; sin embargo, los procesos y procedimientos de control deben ser establecidos e implementados por todo el personal, para así garantizar el cumplimiento de las políticas internas con relación al sistema de administración de riesgo. Sus principales elementos podrían incluir:

- Revisión del avance de los objetivos establecidos.
- Verificación del cumplimiento de los controles establecidos.
- Políticas, procesos y procedimientos con respecto a la revisión, tratamiento y resolución de problemas de incumplimiento.
- Un sistema de aprobaciones y autorizaciones documentadas con el fin de asignar la responsabilidad al nivel apropiado de administración.

Aunque un marco general de políticas y procedimientos es lo más apropiado, esto requiere de ser reforzado mediante una fuerte cultura de control que promueva prácticas adecuadas de gestión de riesgos y prácticas internas para controlar el riesgo operativo; entre ellas podemos citar: el monitoreo cercano relacionado con el cumplimiento de límites de riesgo establecidos, mantener mecanismos de seguridad para el acceso y uso de cierta información confidencial en la empresa, de esta forma aseguramos que el personal tiene las habilidades, experiencia y capacitación apropiadas.

Este marco, incluido en el plan de seguridad de la empresa, supone el desarrollo de los objetivos estratégicos identificados en las políticas y normas de seguridad de la organización, cuya finalidad es ubicar a la entidad a nivel global, en un entorno de riesgo aceptable; resumiendo, el plan de seguridad es el camino que sirve para guiar los pasos de la organización en el cumplimiento de sus objetivos de seguridad.

La definición de políticas, estándares y procedimientos, dentro del marco del plan de seguridad son:

- *Políticas de seguridad informática: Su* propósito es informar a todos los usuarios sobre las expectativas de administración relacionadas al uso apropiado de la información, los sistemas y los recursos.
- *Estándares: Aseguran* que los individuos operan de manera constante, conforme a los estándares para minimizar riesgos, desarrollando una administración de sistemas y redes más eficiente. Son diseñados para una operación consistente y más eficiente.
- *Procedimientos*: Procesos y operaciones que proporcionan los detalles específicos de cómo realizar acciones particulares (mantenimiento, respaldos, manejo de bitácoras, etc.)
  Algunas de sus características, son:

  - Los procedimientos definen cómo se protegerán los recursos y los mecanismos para hacer cumplir las políticas, mientras que las políticas sólo definen que será protegido.
  - Los procedimientos definen a detalle las acciones a tomar en caso de incidentes específicos.
  - Los procedimientos proporcionan una referencia rápida en el momento de un incidente.
  - Los procedimientos eliminan el problema de que un empleado clave esté ausente cuando ocurra un incidente de seguridad.

El siguiente esquema 4.1. Políticas, estándares y procedimientos, muestra la estrecha relación que tienen estas tres.

Esquema 4.1. Políticas, estándares y procedimientos.

Por lo tanto, el objetivo de un Plan de Seguridad es identificar y planificar las políticas y procedimientos, para poder plasmarlos y gestionarlos. Sin embargo muchos de los riesgos podrán ser reducidos mediante la aplicación de un único procedimiento de baja complejidad como por ejemplo, la implantación de un sencillo antivirus, aunque en numerosas situaciones no bastará con una actividad sencilla y habrá que diseñar proyectos específicos para afrontar riesgos complejos.

4.4. Tratamiento de riesgos en Tecnologías de Información

El proceso de tratamiento de riesgos consiste en seleccionar y aplicar las medidas más adecuadas, con el fin de poder modificar el riesgo, para evitar de este modo los daños a los activos de la empresa.

Para que el tratamiento de los riesgos sea efectivo, es necesario que la organización adopte determinadas medidas y acciones encaminadas a reducir, aceptar, evitar o transferir el riesgo. Dichas medidas o acciones, tienen un costo que debe ser asumido por la organización. Del mismo modo, si se decide no adoptar ninguna medida contra el riesgo, pueden existir importantes pérdidas.

A continuación se explica cada uno de los posibles tratamientos.

4.5.1. Aceptar el riesgo

Aceptar el riesgo es una de las técnicas más comunes del tratamiento de riesgos, es la decisión de aceptar las consecuencias de la ocurrencia del evento. Puede ser voluntaria o involuntaria, la voluntaria se caracteriza por el reconocimiento de la existencia del riesgo y el acuerdo de asumir las perdidas involucradas, esta decisión se da por falta de alternativas. La retención involuntaria se da cuando el riesgo es retenido inconscientemente.

Para aceptar un riesgo, primero hay que establecer cuáles son los niveles de tolerancia, así como los objetivos de la seguridad de la información que estamos asegurando, teniendo en cuenta los fines y los requisitos de negocio, legales y contractuales en cuanto a seguridad y de esta manera se puedan establecer criterios de aceptación de riesgo que sean aprobados por los directivos.

Si una empresa adopta la postura de aceptar el riesgo, se debe considerar cuidadosamente quién puede asumir el riesgo, más aún con los riesgos de TI. Los riesgos de TI deben ser aceptados por la dirección de la empresa con la colaboración y el apoyo del área de TI. Si un riesgo particular es evaluado por ser extremadamente raro, pero trascendental y los enfoques para reducirlo son prohibitivos, la administración puede decidir aceptarlo.

4.5.2. Reducir o controlar el riesgo

Reducir el riesgo es la alternativa cuando éste no puede evitarse por tener varias dificultades de tipo operacional. Esta opción es la más económica y sencilla. Se consigue optimizando los procedimientos, la implementación de controles y su monitoreo constante.

El proceso de evaluación del riesgo permite a la organización determinar el grado de exposición de sus activos y definir una estrategia orientada a reducir el mismo. Esta estrategia consiste en llevar a la práctica determinadas acciones que debe adoptar la organización, con el fin de reducir la probabilidad o el impacto del riesgo identificado, o ambos conceptos en forma simultánea.

Para realizar esta estrategia se requiere la creación de tres tipos de planes: el plan de respuesta a incidentes, el plan de recuperación de desastres y el plan de continuidad del negocio. Cada uno de estos planes depende de la habilidad para detectar y responder a un incidente tan rápido como sea posible.

La reducción del riesgo se inicia con la detección temprana de un incidente en progreso y la respuesta efectiva, rápida y eficiente.

- *Plan de respuesta a incidentes. S*on las acciones que una organización puede y debe tomar en caso de un incidente en progreso. El contenido del plan propone las tareas que debe tomar el administrador del sistema cuando ocurre un incidente, lo que permite a la organización realizar acciones coordinadas que sean predefinidas y específicas al evento, ya sean reactivas o correctivas.
- *Plan de recuperación a desastres.* Es el más común de los procedimientos de mitigación o reducción de riesgos; el cual contiene estrategias de respaldo que limitan las pérdidas antes y después de un desastre; así también contiene todos los preparativos para la recuperación de desastres y los pasos detallados a seguir una vez que el desastre haya ocurrido.
- *Plan de continuidad del negocio.* Este plan es el más estratégico y de mayor alcance de los tres mencionados, incluye la planeación necesaria para asegurar la continuidad del negocio, cuando el desastre sobrepasa la habilidad del plan de recuperación de desastres. Desastres como por ejemplo, la pérdida de una base de datos completa o centros de operaciones. El principal objetivo de este plan es que el negocio continúe operando con la mínima interrupción de sus servicios.

4.5.3. Evitar el riesgo

El riesgo es evitado cuando la organización rechaza aceptarlo, es decir, no se permite ningún tipo de exposición y se logra simplemente con la eliminación de las actividades que generan riesgos. Esta técnica tiene más desventajas que ventajas, por lo que la empresa se abstendría de aprovechar muchas oportunidades y probablemente no cumpliría con los objetivos propuestos.

Evitar el riesgo se adopta, generalmente, cuando no se identifica alguna opción de respuesta para reducir la probabilidad o el impacto de un evento.

4.5.4. Transferir el riesgo

El riesgo puede ser transferido de una organización a otra, la cual tenga mayor capacidad de tratarlo, como es el caso de los contratos de seguros o a través de otros medios que permitan distribuir una porción del riesgo con otra entidad; esta técnica es semejante a compartir el riesgo, la diferencia es que al transferir el riesgo, se cede todo, en cambio al compartirlo, la organización responde por una parte del mismo. Por lo tanto la probabilidad o el impacto del riesgo se ve reducido cuando se transfiere o se comparte una parte de este a un tercero.

La estrategia de trasferir pretende trasladar el riesgo a otros activos, otros procesos u otras organizaciones; esto se logra replanteando la forma en que son ofrecidos los servicios, revisando los modelos de ejecución, contratando seguros o implementando contratos de servicios con proveedores.

Transferir el riesgo puede ser implementado en el momento en que una organización empieza a expandir sus operaciones. Si una organización no cuenta con la experiencia en su administración de seguridad, debería contratar personas o firmas que provean tal experiencia, de esta forma puede ser más conveniente contratar servicios integrales, que dedicarle recursos adicionales para desarrollarlos por sí mismos y que representen una mayor inversión.

CAPÍTULO 5

UNA METODOLOGÍA DE ANÁLISIS Y EVALUACIÓN DE RIESGOS EN TECNOLOGÍAS DE INFORMACIÓN

CAPÍTULO 5

UNA METODOLOGÍA DE ANÁLISIS Y EVALUACIÓN DE RIESGOS EN TECNOLOGÍAS DE INFORMACIÓN

5.1. La necesidad de una evaluación de riesgos de seguridad en TI.

Actualmente, las organizaciones dependen en su totalidad de tener la información exacta en el momento preciso; las compañías que no son capaces de alcanzar esto, están en peligro de extinción, porque con el paso de los años, la información se ha convertido en el elemento de mayor importancia para la toma de decisiones. Y es aquí donde radica la prioridad de desarrollar nuevas tecnologías que permitan tener la información requerida y oportuna para ser utilizada. Sin embargo, la mayoría de las empresas han fallado al no aprovechar el ambiente existente e implementar ideas innovadoras para mejorar el papel que juegan las tecnologías de información dentro de sus organizaciones

La información contenida en los sistemas de cada empresa debe ser protegida y preservada, para ello es necesario hacer un estudio real de las amenazas y de las formas en que las mismas pueden ser reducidas. Por esta razón, el presente capítulo tiene como meta el definir una metodología que cubra los aspectos fundamentales que se deben considerar en el análisis, evaluación y administración de riesgos de Tecnologías de Información en todas las empresas.

Una evaluación de riesgos toma muchos nombres y puede variar conforme a los términos del método utilizado, dependiendo el rigor con el que es realizado y el alcance de dicha evaluación, pero el objetivo principal es siempre el mismo: evaluar los riesgos de seguridad que ponen en peligro los activos de información de la organización. La información obtenida por esta evaluación es usada para determinar de qué manera atenuar los riesgos de seguridad encontrados y preservar de la mejor forma el objetivo de la organización.

Los beneficios que presenta una evaluación de riesgos de seguridad en Tecnologías de Información son los siguientes:

- *Definición de la situación actual*. Una evaluación de riesgos proporciona a la organización el estado actual de la protección de sus activos de información, que servirá como base para iniciar trabajos adicionales a fin de proteger dichos activos. En esta evaluación, el trabajo del administrador de seguridad de la información y el grupo de operaciones de seguridad serán revisados por un grupo externo, el cual tendrá como objetivo el determinar la precisión del programa de seguridad y hacer ver las áreas de mejora.
- *Revisiones periódicas*. El programa de seguridad de información diseñado de la manera más cuidadosa, requiere de revisiones periódicas. Estas revisiones proveen un porcentaje de la efectividad del programa ya implementado dentro de la compañía y dan la información necesaria para ajustarlo a las cambiantes amenazas a las que está expuesta la organización.

- *Costo del Riesgo.* La asignación de los recursos al programa de seguridad puede basarse en los riesgos de seguridad de los activos encontrados en la evaluación. Las organizaciones generalmente cuentan con recursos limitados para asignarlos a los problemas que surjan en la seguridad de la información, de no realizarse una evaluación de riesgos, éstas no tendrán el conocimiento de las amenazas en los activos de información.
- *Requerimientos legales o de operación.* Una evaluación de riesgos de seguridad en una institución privada o gubernamental, es un requerimiento necesario que se aplica para que dicha organización trabaje bajo ciertas normas legales o de operación de seguridad.

5.2. Objetivo general del análisis de riesgo

El objetivo general del análisis de riesgo es evaluar la efectividad de los controles de seguridad, que protegen a los activos de la empresa y determinar la probabilidad de pérdida de estos.

El análisis de riesgos investiga las amenazas dentro de una organización: el valor de los activos, la criticidad de los sistemas, las vulnerabilidades en los controles de la seguridad y el impacto posible por la pérdida; además recomienda controles adicionales para reducir el riesgo a un nivel aceptable.

5.3. Propuesta de una metodología de análisis y evaluación de riesgos en Tecnologías de la Información.

5.3.1. Definición del proyecto.

El éxito en el análisis y evaluación de riesgo recae tanto en las habilidades y la experiencia del grupo asignado, como en la efectividad del plan de seguridad. Dentro de la fase de definición del proyecto, éste debe ser apropiadamente definido en cuanto a su alcance y claramente documentado en la organización, establecido en un posible contrato entre ésta y la empresa consultora.

El alcance en cualquier proyecto debe tener claro el costo y tiempo estimado para llevarse a cabo. El líder del grupo necesita asegurarse que el presupuesto para el proyecto y el tiempo requerido sean aceptados por la organización. La aceptación de estas variables deberá documentarse y será incluida en el plan del proyecto.

El plan del proyecto documenta tanto el presupuesto y tiempos requeridos, como divide la evaluación y análisis en tareas manejables, asignando los recursos requeridos. El esquema del proyecto se presenta en la siguiente figura 5.1.

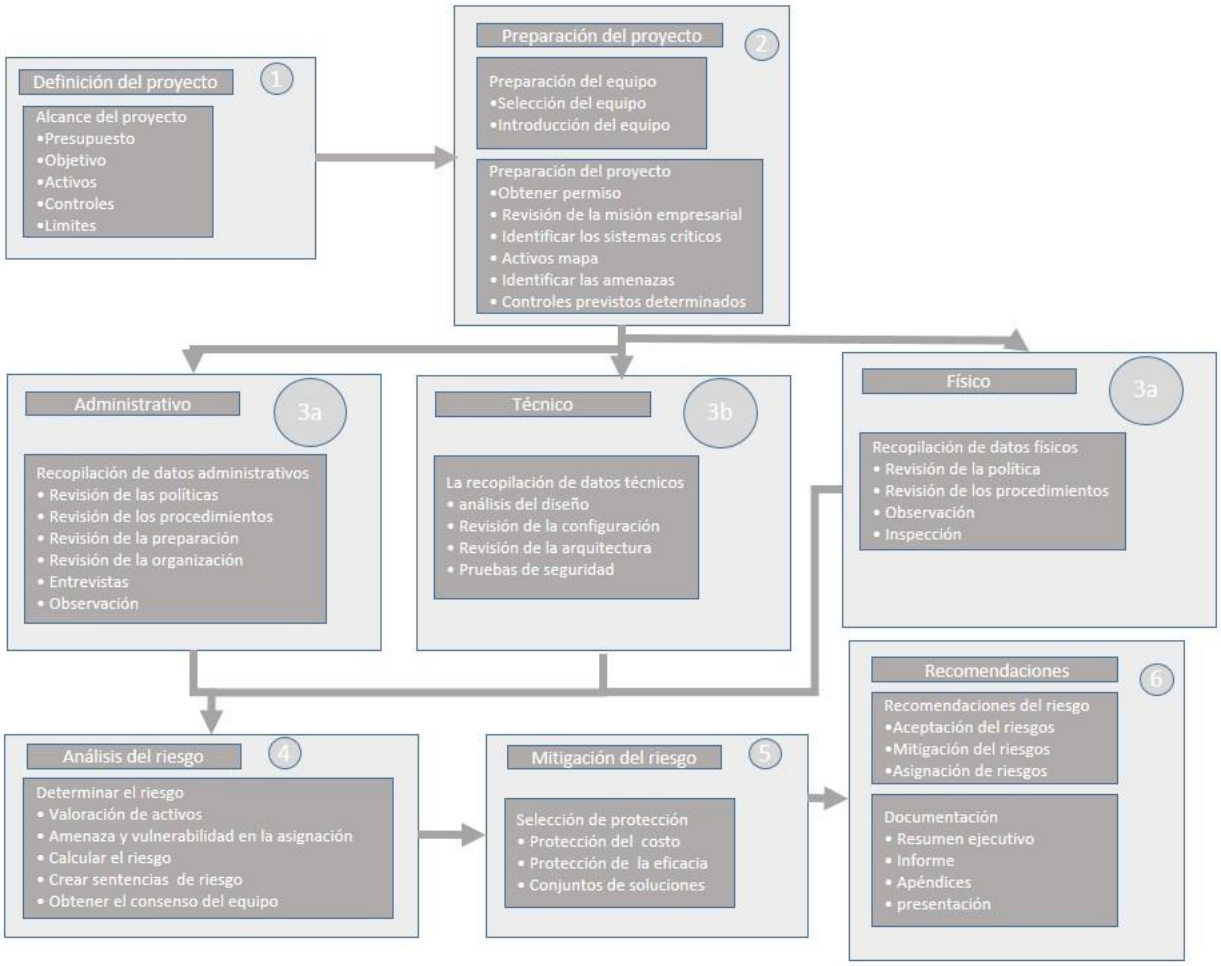


Figura 5.1. Esquema del Proyecto

Sin considerar el presupuesto y el tiempo requerido, el alcance del análisis y la evaluación de riesgos puede ser más complejo que el alcance de otros proyectos. El tener definido el objetivo del análisis y la evaluación de riesgos es necesario para entender las necesidades de la organización. Por ejemplo, la evaluación que se realiza para cumplir con los requerimientos de una ley, tiene un objetivo diferente del que se efectúa para asegurar el cumplimiento de un programa de seguridad. El grupo debe tener claros los límites de la evaluación a través de la identificación de los activos, sistemas y otras limitantes en el proyecto.

Uno de los factores principales para un adecuado alcance en una evaluación de riesgos es el presupuesto asignado. En caso de que este rubro no exista debe tomarse en consideración cuánto se está dispuesto a invertir, no se requieren de números exactos, pero hay una enorme diferencia en el alcance y en el rigor en una evaluación de riesgos de cinco millones de pesos a una de quinientos mil pesos. El hecho es que mientras más tiempo pase un grupo revisando los controles de seguridad, más rigurosa será la evaluación.

Conjuntamente con el rigor en el análisis, el monto económico que se planee invertir en la evaluación de riesgos se verá afectado por: el tamaño de la organización, la distancia geográfica de los elementos organizacionales, la complejidad de los controles de seguridad y las amenazas en el medio ambiente a las que esté expuesta. Cada organización opera dentro de un nivel de seguridad propio; por ejemplo, un laboratorio farmacéutico internacional claramente está expuesto a riesgos más serios que las oficinas corporativas de una franquicia de café.

5.3.2. Preparación del proyecto.

Con base en el alcance del proyecto de evaluación de riesgos identificado en el inciso anterior 5.3.1, el líder de proyecto necesita asegurar la integridad del negocio, ya que se prepara para iniciar con la recolección de datos. Como parte de esta preparación, se debe considerar, tanto la selección de los miembros del grupo que participará en la evaluación, como en la presentación de éste con los directivos de la organización que va a ser evaluada; en caso de que la empresa contrate los servicios de otra para dicha evaluación o que los empleados de la misma sean quienes la realicen.

Muchos factores influyen en esta fase para la correcta selección del grupo, entre ellos se incluye la objetividad, la experiencia y el conocimiento de los miembros seleccionados. Además se debe considerar el uso de cartas de presentación formales ante el cliente, de igual forma las solicitudes formales de accesos y permisos que se requieran.

5.3.3. Recolección de datos administrativos.

La recolección de datos es realizada en las instalaciones de la organización a ser evaluada, y da como resultado la información acerca de la efectividad de los controles de seguridad técnica, física y administrativa actuales. El grupo de seguridad revisará los controles respectivos a través de la colección, revisión y análisis de las políticas, normas y procedimientos establecidos por la empresa; además de la observación y entrevistas a su personal.

5.3.4. Recolección de datos técnicos.

En esta etapa, los datos recabados acerca de los controles de seguridad física, nos servirán para que dichos controles sean evaluados a través de la observación, las pruebas y el análisis. En forma similar, la evaluación de los controles de seguridad técnicos, serán evaluados a través del análisis técnico, las pruebas de dichos controles y la revisión de las bitácoras de operación. Esta etapa es decisiva en el proyecto, junto con la recolección de datos administrativos y posiblemente se ampliará más adelante.

5.3.5. Análisis de riesgos.

En esta fase del proyecto, los datos obtenidos y su posterior análisis, nos proporcionan un panorama amplio de los riesgos a los que la organización está expuesta. Es en esta fase, que el grupo de evaluación de riesgos de seguridad debe determinar el valor de: los activos de la empresa, la criticidad de los sistemas, las posibles amenazas y la existencia de vulnerabilidades basadas en los datos recolectados. Adicionalmente a las actividades antes descritas, el grupo debe calcular los riesgos de la organización para cada amenaza o vulnerabilidad, presentando estos datos en función del método de evaluación de riesgos de seguridad seleccionado.

5.3.6. Mitigación de riesgo.

El grupo deberá desarrollar las recomendaciones para reducir los riesgos a un nivel aceptable dentro de una organización, basándose en riesgos definidos en el inciso anterior. La selección de las medidas de mitigación se ajustará a cada dupla de amenaza o vulnerabilidad, determinando la reducción del riesgo, el costo de la mitigación de éste y se agruparán en conjuntos de soluciones.

5.3.7. Reporte de riegos y recomendaciones.

En esta última fase, el grupo de evaluación de riesgos presentará un reporte al cliente o al usuario clave, el cual identifica claramente los riesgos encontrados y las mitigaciones sugeridas. Este reporte debe incluir información clara para los ejecutivos de la empresa, el grupo gerencial y el personal técnico. Las recomendaciones para mitigar los riesgos encontrados, son finalmente el punto principal de toda evaluación de riesgos.

5.4. Definición del proyecto

Para que un proyecto de evaluación de riesgos pueda ser calificado como exitoso, primero debemos definir qué entendemos por exitoso. Para este propósito, definimos el éxito del proyecto como la satisfacción del cliente o la organización con el trabajo realizado, el trabajo técnico entregado con calidad y la conclusión del proyecto dentro del presupuesto previamente acordado.

5.4.1. Identificando al cliente

El cliente en un proyecto de análisis y evaluación de riesgos en Tecnologías de Información, incluye al patrocinador y a interesados dentro de la organización a ser evaluada. Estos tienen diferentes puntos de vista y opiniones, por lo tanto, deben ser considerados para alcanzar el éxito del proyecto.

Cuando una evaluación de riesgos es realizada con recursos internos de la empresa y comisionada a una consultoría de seguridad, el cliente principal del proyecto es aquella persona responsable de la contratación. En el caso de que la evaluación sea interna, el patrocinador del proyecto será el gerente del departamento o el director que hubiere asignado a este gerente.

Se hace énfasis en la definición del patrocinador del proyecto, debido a que es él, el responsable interno del mismo. En el caso de que se contrate a una consultoría, entonces el patrocinador del proyecto será quien firme la autorización para realizar éste. En cualquier caso, el patrocinador del proyecto es quien definirá el éxito del proyecto en términos de la calidad del trabajo técnico efectuado, dentro del tiempo y presupuesto establecido.

Los clientes secundarios de un proyecto de análisis y evaluación de riesgos, incluyen a los interesados en el proceso y juegan un papel importante en la aceptación final de la evaluación y por lo tanto en la satisfacción del cliente principal. Los clientes secundarios vienen siendo:

- *El grupo de seguridad.* Puede ser desde el oficial de seguridad de mayor rango, con su grupo incluido y presupuesto de seguridad, o un administrador de sistemas con el control de los parámetros de red, dependiendo de la complejidad de la organización.
- *Gerentes de las unidades de negocio.* Las organizaciones dividen su responsabilidad para la gobernabilidad de la corporación en unidades de negocio. Estas unidades de negocio pueden ser: grupos, departamentos, divisiones o direcciones; que a su cargo se encontrará un solo individuo conocido como el jefe de división, director o gerente.

  Deben tomarse en cuenta las siguientes recomendaciones para tratar con estos clientes.

  - *Entender a las unidades de negocio.* Los responsables de las unidades de negocio son quienes tienen el conocimiento de cómo funciona la entidad, la identificación precisa de riegos de seguridad, las recomendaciones útiles y son quienes conocerán el costo de la implementación de estas. Por lo tanto es importante entender y conocer el funcionamiento de las unidades de negocio, pues al hacerlo y considerar sus opiniones, nos ayudará a que sean aceptados los resultados que se entreguen en los documentos finales.
  - *Identificación precisa de los riesgos de seguridad.* Los gerentes de las unidades de negocio son quienes normalmente generan las críticas más severas a los resultados de los proyectos de evaluación que afectan a las unidades de negocio, siendo que estos resultados y sus recomendaciones influyen directamente en el presupuesto de sus unidades de negocio. Por ello, el grupo del proyecto debe asegurarse que la identificación de los riesgos de seguridad sean puntuales.
  - *Precisión y utilidad de las recomendaciones*. El componente más valioso de una evaluación de seguridad es una lista priorizada de acciones a tomar para reducir los riesgos de seguridad. Una evaluación que sólo indique que la organización se encuentra en un cierto nivel de seguridad no es de utilidad. Si únicamente se incluyen recomendaciones ambiguas, como “aumentar el personal de seguridad”, lo cual es poco preciso y claro, brindan poca guía a quienes deben actuar conforme a las recomendaciones.

- *Costo de implementación de las recomendaciones.* Los gerentes de las unidades de negocio prefieren escuchar que las medidas de seguridad serán fáciles y baratas de implementar, esto es contraproducente. Es preferible que aunque se cause incomodidad inicial por el costo de las recomendaciones, éstas sean lo más precisas posibles pues al final el costo real de las implementaciones puede causar una molestia aún mayor.

➢ *Responsable del cumplimiento del departamento legal***.** Una evaluación de seguridad es para muchas organizaciones un requerimiento legal. En estos casos, quien sea responsable del cumplimiento de las políticas, normas y procedimientos aplicables dentro de la organización, es quien será el más interesado en los métodos y resultados de la evaluación. Para este punto, deberá considerarse lo siguiente:

- *Método usado.* En el caso de que la evaluación sea solicitada para cumplir con algún requerimiento legal, el cliente puede tener requerimientos estrictos que deben ser cumplidos en cuanto a la metodología establecida. Por esto, el líder de proyecto de evaluación debe estar familiarizado con las regulaciones que apliquen y solicitar de manera explícita que en el contrato se especifiquen los requerimientos que se deban cubrir para realizar la evaluación.
- *Grupo de evaluación de riesgos de seguridad.* Aunque las regulaciones existentes no piden explícitamente seguir un método, si tienen requerimientos indirectos acerca de la objetividad y los conocimientos de los miembros del grupo del proyecto de evaluación.
- *Revisión objetiva*. Es necesario que la evaluación conserve la objetividad suficiente para evitar conflictos de interés aparentes o reales. El conflicto ocurre cuando algún miembro del grupo de evaluación quiere llegar a un resultado específico o cuando algún miembro del programa de seguridad es evaluado, como los arquitectos de seguridad o los encargados de los controles físicos. Este personal pudiera tener algún interés en presentar los hallazgos de una manera desviada.
- *Credenciales de los miembros.* Los miembros del grupo de seguridad deben tener cierto nivel de experiencia, que les permita comprender los conceptos que se aplican en la evaluación de seguridad y con base en sus conocimientos, ser miembros productivos del grupo y actuar profesionalmente.

  Un miembro del grupo de seguridad sin conocimientos básicos y cierta experiencia, puede desviarse de los objetivos planteados o malinterpretar los resultados y no ser de utilidad para el proyecto. El grupo requiere de miembros con experiencia en el campo, para evaluar adecuadamente la frecuencia de las amenazas, el impacto y los riesgos en la seguridad

- *Técnicos, operadores y administradores***.** Es el personal que mantiene y opera los controles de seguridad de la organización; aplica los parches de seguridad, mantienen los perfiles de los usuarios y la información de sus cuentas; también establece las reglas de operación de los firewalls, entre otras actividades. Estos empleados tiene mayor interés en la calidad que se perciba de su trabajo, ya que una evaluación de riesgos puede ser muy estricta y encuentre fallas en lo realizado por el empleado. Aunque no son el cliente a satisfacer, ellos influyen en gran medida en el cliente principal, por lo que los hallazgos deben ser precisos y cuidadosamente escritos, procurando no señalar culpables, sino su impacto potencial y como solucionar los riesgos.

5.4.2. Calidad del trabajo.

Los clientes basarán la apreciación del proyecto en los resultados plasmados en el reporte final; por lo que el grupo de seguridad debe tener bien claro el objetivo primario, ya que en muchas ocasiones se da prioridad a las actividades técnicas y se descuida entregar el reporte con calidad al patrocinador del proyecto.

Los aspectos de calidad más relevantes en la presentación del reporte final son:

- *Gramaticalmente correcto.* Toda correspondencia que llegue al cliente, es una representación del autor y la organización que personifica. Por lo tanto un documento formal del proyecto puede ser un reporte o inclusive un borrador, los cuales deben ser correctos en su sintaxis y gramática. Aunque no debería ser un factor decisivo, la impresión que tenga un cliente del trabajo escrito es tan importante como el análisis contenido en dicho reporte.
- *Visualmente agradable.* Se recomienda que los entregables tengan un formato uniforme y consistente, pues denotara experiencia y profesionalismo Los siguientes puntos deben ser considerados dentro de la elaboración del reporte:

  - Seleccionar el mismo tipo de letra para todo el reporte.
  - Elaborar de manera consistente las tablas, dibujos, listas, etc.
  - Se deben usar estilos para los encabezados que sean adecuados al reporte.
  - Debe cuidarse el uso apropiado de encabezados y pie de páginas.

- *Dirigido a quien deba tomar las decisiones.* El reporte final debe cubrir diferentes puntos de vista y niveles de experiencia, por lo que debe ser escrito pensando en todos los involucrados, es recomendable cuidar los siguientes aspectos:

  - *Resumen ejecutivo.* Debe ser escrito para los involucrados que necesitan saber lo más relevante, ser corto y directo, además de contestar a la pregunta: ¿Cuáles son los riesgos de seguridad en mi administración y que se debería hacer al respecto?

- *Apéndices técnicos.* Las especificaciones técnicas y la documentación de soporte de la evaluación de seguridad, deben incluirse en este apartado. Los lectores más técnicos querrán los detalles relativos a la vulnerabilidad o la lista de los usuarios con contraseñas fáciles de descifrar. A continuación listamos algunos de los apéndices más comunes que debe contener un reporte de seguridad.

  - *Identificación de vulnerabilidad.* Los resultado de los escaneos realizados en los sistemas evaluados.
  - *Evidencias*. Una lista de evidencias, tales como las entrevistas realizadas, el resultado de las pruebas, documentos en hojas de cálculo, etc.
  - *Referencias.* Una lista de fuentes de información y guías usadas en el proceso de evaluación.
  - *Descripción de soluciones*. Descripciones adicionales a las soluciones propuestas
  - *Cálculos*. Cálculos matemáticos que apoyen los hallazgos.

- *Entendimiento del tema*. Es importante que el lector del reporte se dé cuenta a través del contenido, que el grupo de la evaluación de riesgos tiene el conocimiento para ejecutar las pruebas y la formación necesaria para realizar el trabajo. En la introducción del reporte puede incluirse información relevante de la empresa, concerniente a la evaluación, así como la necesidad para realizar dicha evaluación.

5.4.3. Presupuesto.

Uno de los factores más importante en cualquier proyecto, es que éste sea terminado en tiempo y forma, dentro del presupuesto establecido. Es responsabilidad del líder del grupo de evaluación, administrar el tiempo y los recursos asignados. Cualquier proyecto que no sea completado dentro del tiempo y presupuesto establecidos puede que sea cancelado o cumplido demasiado tarde representando una desventaja al negocio, haciendo notar la falta de experiencia del grupo evaluador.

Definir el presupuesto, es un factor importante para calcular el alcance de una evaluación y cuál será el costo en la evaluación requerida. Si este factor no está limitado, entonces se debe establecer cuánto se quiere gastar; existe mucha diferencia entre gastar cuatro millones de pesos o 400 mil pesos, ya que entre más tiempo y dinero se invierta en revisar los controles de seguridad, más rigurosa será la evaluación realizada. Además, mientras más dinero se dedique al proyecto, mayor será el rigor exigido en los hallazgos y en el reporte final.

Los factores que más influyen en la definición del presupuesto son:

- *Tamaño de la organización.* Mientras más grande sea la organización, mayor será la cantidad de controles que deban ser revisados, a diferencia de una organización de menor tamaño, en la que su estructura sea sencilla y limitada a tal vez una sola localidad.
- *Separación geográfica.* Una organización con múltiples oficinas, sistemas y personal, geográficamente separados, requerirá de un mayor presupuesto, debido a los costos adicionales a los viáticos para la recolección de la información.
- *Complejidad.* En este punto es conveniente considerar que tan complejos son los sistemas con los que cuenta la empresa por evaluar. Mientras más complejos sean los sistemas de control, se requerirá mayor esfuerzo para que éstos sean evaluados con efectividad. Si la empresa, por ejemplo, cuenta con controles de acceso físico que incluyen bardas perimetrales, guardias armadas, controles de seguridad biométricos, un sistema de circuito cerrado de TV, accesos con tarjetas inteligentes y algún otro sistema de detección de intrusos, se necesitará de un mayor esfuerzo para realizar una revisión efectiva de todos estos controles, y por lo tanto se incrementará el costo de la evaluación de manera proporcional a los sistemas por evaluar.
- *Amenazas del medio ambiente.* Debe considerarse el medio ambiente en el que trabaja la organización por evaluar; por ejemplo, en el caso de una empresa farmacéutica, estará expuesta a un rango de riesgos más amplio y deberá cumplir con reglamentaciones, posiblemente, más severas que el corporativo de una cadena de restaurantes.

Se considera entonces que una organización podrá dedicar únicamente una porción de su presupuesto para seguridad en una evaluación. Aunque debería ser normal, no siempre es considerado. Si una organización invierte la mayoría de su presupuesto para seguridad en una evaluación exhaustiva, en un período fiscal determinado, puede quedarse sin la posibilidad de realizar las recomendaciones finales de la evaluación.

5.4.4. Determinando el objetivo.

Un proyecto de análisis y evaluación de riesgos de seguridad ofrece importantes beneficios, tales como:

- Una base para la disminución del gasto enfocado en los riesgos.
- Una revisión periódica del programa de seguridad establecido.
- Una confirmación de los procedimientos ya establecidos para las tareas delicadas que realice la organización.

El entender y documentar el objetivo que se busca con la evaluación, ayuda a enfocar los procesos para satisfacer puntualmente las necesidades de la organización.

5.4.5. Definición del alcance de la evaluación de seguridad.

La definición del alcance de evaluación de seguridad está a cargo del patrocinador y su grupo, que delimitan con claridad y cuidado el alcance en función de los controles a revisar y los activos a proteger. La identificación de los límites del proyecto es esencial para que el grupo de evaluación se asegure que el alcance no se sobredimensione o que los límites establecidos no satisfagan las necesidades de la empresa.

5.4.5.1. Definición de un bajo alcance de seguridad.

El definir un bajo alcance de seguridad, no contempla todos los aspectos que requiere el patrocinador. Por ejemplo, no incluir algunos activos de la organización o no contemplar amenazas relevantes dentro del análisis de riegos provocara que los activos de la dependencia queden expuestos.

5.4.5.2. Definición de un elevado alcance de seguridad.

Definir un elevado alcance de seguridad, puede cubrir amenazas, vulnerabilidades o riesgos que sobrepasan las necesidades del patrocinador en la evaluación. Por ejemplo, sobrepasar la autoridad concedida al grupo de evaluación después de haber probado sistemas que no estén explícitamente definidos en dicha autoridad.

5.4.5.3. Controles de seguridad.

Normalmente una organización implementa una amplia variedad de controles de seguridad para proteger sus activos, estos controles de seguridad pueden ser políticas y procedimientos, soluciones anti-virus y firewalls. Para facilitar la definición del alcance de la evaluación de seguridad, es recomendable agrupar estos controles en tres categorías, a saber: administrativas, físicas y técnicas.

- *Controles de seguridad administrativos*. Son definidos como políticas, normas y procedimientos para proteger los activos de la organización.
- *Controles de seguridad físicos*. Están asociados a la protección de los empleados e instalaciones de la organización, pueden incluir bardas perimetrales, vallas, puertas, controles de acceso, guardias y CCTV, además de procedimientos en caso de eventos de la naturaleza y de evacuación.
- *Controles de seguridad técnicos*. En este apartado se contemplan los mecanismos para proteger de manera lógica los activos de la organización, tales como: ruteadores, corta fuegos, soluciones anti-virus, controles lógicos de acceso y los sistemas de detección de intrusos (IDS). La evaluación debe considerar las capacidades de los controles de seguridad técnicos, sus configuraciones actuales y los sistemas para la protección de los activos.

Para el propósito de éste trabajo, los activos de una organización son los recursos a través de los cuales la organización genera valor. Estos pueden incluir: hardware, software, sistemas, servicios, documentos, propiedades personales, gente, secretos industriales, formulas, y cualquier otro elemento del proceso del negocio; para una organización, no siempre es fácil definir qué es un activo y qué no lo es, por ello, consideramos como activos tangibles e intangibles a los siguientes:

- *Activos tangibles*. Son aquellos que "se pueden tocar", como el hardware (o equipo), sistemas, redes, interconexiones, telecomunicaciones, cableado, mobiliario, registros de auditoría, libros, documentos, efectivo y software. Sin embargo, el activo número uno, siempre lo serán las personas (empleados, proveedores, clientes, invitados, visitantes y otros). Estos activos son los que pueden ser más fácilmente listados, pues son visibles e inclusive contabilizados dentro de registros de auditoría.
- *Activos intangibles*. Son aquellos que "no se pueden tocar", tales como la seguridad y salud de los empleados, datos, privacidad del empleado y del cliente, imagen y reputación de la organización. Dichos activos son difíciles de listar o enumerar, pues no son visibles o contables en registros.

5.4.5.4. Identificación de los límites en los sistemas de información.

Es importante considerar los límites en sistemas de información, ya que son el punto de partida para iniciar con la evaluación de seguridad; se considera que un sistema de información es cualquier proceso o grupo de procesos relacionados, generalmente dentro de un mismo sistema operativo. Estos comprenden los procesos, comunicaciones, almacenamiento y recursos necesarios para que el sistema de información opere.

Por lo tanto cada sistema de información a ser evaluado, debe tener identificados de manera explícita sus límites físicos y lógicos.

- *Límites físicos.* Consisten en identificar el entorno material en el que se llevará a cabo la evaluación de seguridad.
  Los elementos por considerar dentro de los límites físicos de un sistema son:

  - Estaciones de trabajo
  - Servidores
  - Equipo de redes
  - Equipo especial
  - Cableado
  - Periféricos (repetidores, estaciones de microondas, etc.)
  - Edificios
  - Pisos dentro de los edificios o habitaciones individuales.

- *Límites lógicos*. Consiste en identificar las funciones de los sistemas informáticos dentro del alcance de la evaluación.

En la figura 5.2. Se muestra el límite de los elementos lógicos en un sistema de Información, indicado mediante líneas discontinuas gruesas y delgadas.

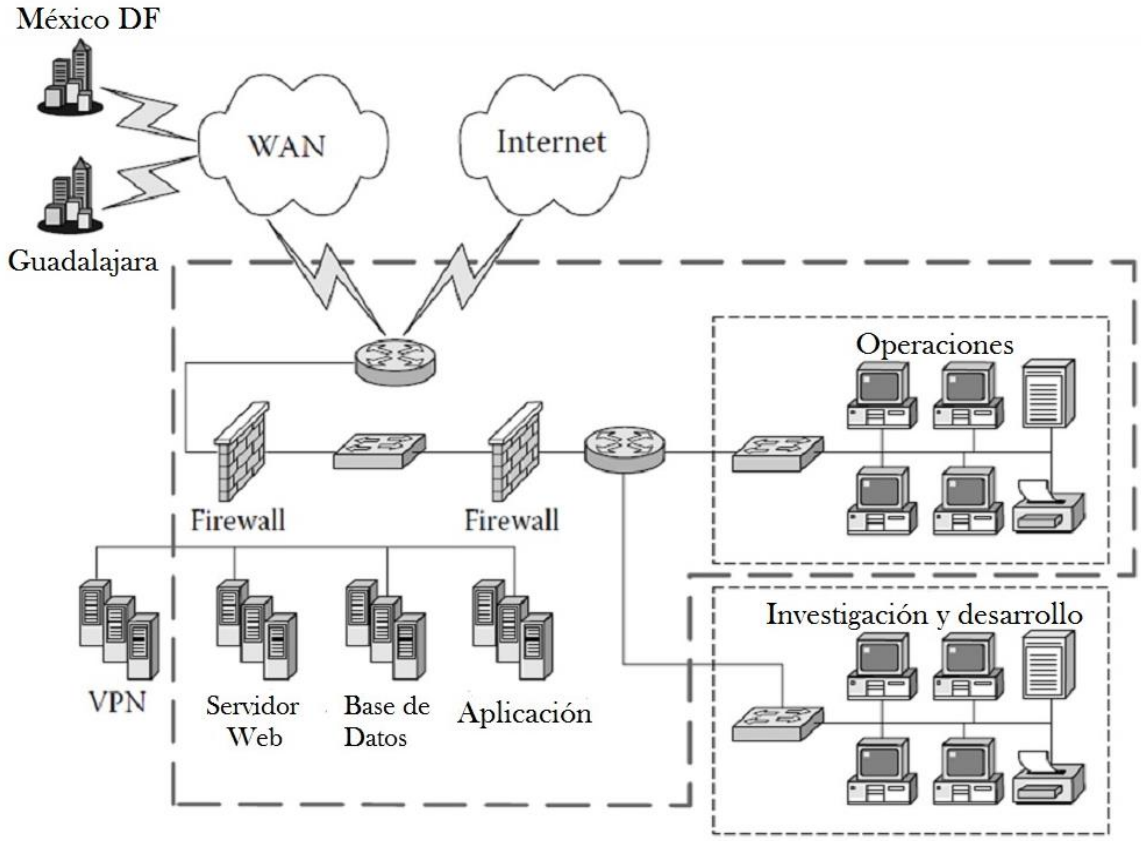


Figura 5.2. Límite de elementos lógicos en un sistema de información.

Una vez que se han identificado los límites de los sistemas de información a ser evaluados, puede ser más sencillo acotar el alcance del proyecto de evaluación. Debe tomarse en cuenta que un sistema sin límites, no puede ser evaluado.

Las únicas razones por las que no se debería incluir algún sistema de información dentro de los límites físicos de la evaluación, serían que estos se encuentren dentro de los siguientes casos:

- Las funciones de los sistemas se identifican como no relevantes para la evaluación.
- La función del sistema identificado ya es parte de otra evaluación.
- El análisis de las funciones del sistema sobrepasen las capacidades del grupo de evaluación.
- Los controles ambientales o físicos hacen que las funciones del sistema sean irrelevantes por la seguridad con la que ya se cuenta.

5.4.6. Entregables.

La descripción del trabajo por realizar puede ser tan extensa como se quiera; para que sea de utilidad al cliente, el reporte de evaluación de riesgos debe establecer con claridad cuatro elementos fundamentales:

- El proceso de evaluación utilizado
- La evidencia que se obtuvo
- Los resultados
- Las recomendaciones

La descripción del proceso utilizado debe ser breve y clara, incluyendo la metodología empleada, dando al patrocinador del proyecto la confianza de que se utilizó la metodología adecuada y una guía para entender los resultados.

5.5. Preparación para la evaluación.

5.5.1. Introducción al grupo de evaluación.

Se recomienda al inicio de la gestión de evaluación, que el grupo encargado sea presentado ante la organización por evaluar, teniendo en cuenta la importancia de la confianza que tenga el cliente en la profesionalidad del grupo de evaluación.

En ocasiones el grupo de evaluación de seguridad es presentado durante el proceso de licitación o negociación, pero de cualquier manera una carta de presentación debe ser utilizada para formalizar el inicio del proyecto de evaluación de seguridad.

5.5.2. Carta de presentación.

La carta de presentación que señala el inicio del proyecto, debe tener ciertos elementos clave, estos son los puntos principales de contacto entre el cliente y el grupo de evaluación, fechas de inicio y finalización previstas para el proyecto, la información requerida y el acceso al centro de datos.

5.5.3 Informe de pre-evaluación.

Un informe de pre-evaluación ayuda a establecer las expectativas de la organización por evaluar y a atender las preocupaciones de ésta; por consiguiente ajustar el enfoque de la evaluación respecto de los resultados que se vallan obteniendo.

El Informe de pre-evaluación debe cubrir los siguientes aspectos:

- *Introducción.* Del grupo de evaluación a la organización, la revisión de los objetivos de evaluación, un calendario de las evaluaciones programadas y la sesión informativa final.
- *¿Qué esperar?* El representante del grupo informará a los miembros de la organización lo que se espera de la evaluación. Se recomienda tomar en cuenta lo siguiente para la interpretación de la evaluación.

    - *Herramienta de planificación.* La organización que está siendo evaluada debe comprender que la evaluación es una herramienta de planificación que determina los riegos y que éstos no necesariamente son indicadores de que el personal está haciendo mal sus labores, sino que la evaluación debe ser percibida como una necesidad para el personal y de que posiblemente se requieran incrementos del mismo, así como del presupuesto de seguridad, tales aumentos como la mejora de los controles existentes, requieren de una planificación. La evaluación de riesgos de seguridad es el primer paso en el proceso de planificación.
    - *Proceso de gestión de riesgos.* La evaluación de riesgos es el primer paso para determinar los nuevos controles de seguridad, sin embargo las pruebas periódicas y controles operacionales juegan un papel muy importante en la gestión de riesgos.
    - *Hallazgos.* Es probable que se identifiquen varios resultados, por lo que la organización no debe sorprenderse por la cantidad de riesgos que se encuentren, sino por el nivel de riesgo que estos presenten.

- *No todas las soluciones serán sencillas.* Algunas de las recomendaciones propuestas de la evaluación, serán de tipo operativo y requerirán una solución sencilla, sin embargo algunos riesgos como las amenazas naturales requerirán una planificación a largo plazo.
- *Información necesaria.* El representante del proyecto de evaluación, debe notificar a la organización que necesitará información sobre los procedimientos de acceso, experiencias pasadas con las evaluaciones; así como, comunicar los posibles cambios en la arquitectura y planes para los controles de seguridad adicionales.

5.5.4 Accesos a los sistemas de información.

Antes de iniciar la recolección de datos, el grupo de evaluación de seguridad debe contar con la autorización apropiada para determinadas actividades de recopilación de datos. Estas actividades incluyen el monitoreo de comunicación de los usuarios y el acceso a los sistemas de información.

5.5.4.1. Políticas requeridas para la evaluación de seguridad.

Si la evaluación de seguridad incluye el monitoreo de la comunicación del usuario, entonces el proyecto deberá asegurar que las actividades que se desarrollen, no violen las leyes aplicables y las regulaciones.

En la mayoría de los casos, las evaluaciones de seguridad no necesitan monitorear: correos electrónicos, correos de voz, o conversaciones telefónicas. La única razón para realizar dichos monitorios, es asegurar a la organización que no hay ningún riesgo por el uso de estos métodos de comunicación.

Algunos de los riegos posibles que se pueden detectar al realizar una evaluación de seguridad, son:

- Usuarios autorizados, podrían estar enviando información no autorizada; v.g. enviar información sensible a un competidor.
- Usuarios autorizados pudieran recibir información no autorizada o archivos v.g. archivos ejecutables con código malicioso.
- En cualquiera de los casos anteriores una revisión a los controles de seguridad establecidos por la organización, darían la certeza al grupo de seguridad de la posibilidad de dichos riesgos.

5.5.4.2. Obtención de los permisos autorizados.

Si el grupo de evaluación planea acceder o intentar el acceso a los sistemas de información de la empresa, entonces se debe asegurar la obtención del permiso autorizado. Esta autorización debe incluir el permiso escrito y explícito del propietario, así como del responsable de los sistemas de información. Deberá tomarse en cuenta que el determinar con exactitud la propiedad del sistema, no es siempre una tarea sencilla.

Como siguiente paso, se debe considerar el que pueden existir múltiples propietarios de los sistemas de información, o de los sistemas intermedios que conectan a la organización con otros sistemas. Por ejemplo, el sitio Web del cliente puede ser hospedado en una instalación de un proveedor del servicio. Amén de que el sitio Web probablemente esté corriendo en un servidor compartido. El grupo puede haber obtenido el permiso del dueño del sitio Web, pero no del propietario del sistema que hospeda al sitio Web. En este caso, el grupo de evaluación estaría cayendo en una falta, si corre procesos de escaneos de vulnerabilidad y penetración contra el sitio Web, posiblemente afectando la operación de otros sitios Web en el servidor compartido.

Por lo tanto es recomendable que el grupo deba asegurarse de tener el permiso del dueño de todos los sistemas que necesitan con objeto de tener acceso para hacer pruebas de los sistemas.

5.5.4.3. Alcance de los permisos obtenidos.

Se recomienda que paulatinamente las organizaciones otorguen permisos para acceder a sus sistemas. Los permisos para las pruebas de seguridad sólo deberán ser otorgados para sistemas definidos y en horarios determinados, exclusivamente para un propósito específico. La forma de los permisos para acceder a los sistemas que se incluyen en las pruebas deberá indicar las direcciones IP y el número telefónico cuando se emplee *war dialing* o ingeniería social.

Por último, es conveniente que el tipo de prueba, esté descrito en los formatos. Por ejemplo, pruebas de vulnerabilidad, pruebas de penetración, ingeniería social, war dialing, entre otros.

5.5.4.4. Tipo de cuentas de acceso requeridas para las pruebas.

El grupo de evaluación de seguridad debe especificar al patrocinador el número y tipo de cuentas de acceso que se requerirán. Las cuentas requeridas para cualquier evaluación de seguridad dependen de los procesos que se usarán por el grupo de evaluación y de los permisos que se requieran para ejecutar dichos procesos.

5.5.5 Entender la misión del negocio

Antes de analizar y dar a conocer los riesgos de la organización, es necesario que el equipo de evaluación de seguridad tenga una comprensión básica de: la misión corporativa, la estructura, los negocios y los objetivos de la empresa, con objeto de identificar los activos de la misma, sus riesgos potenciales y el impacto de éstos sobre sus activos.

5.5.5.1. Información necesaria de la misión del negocio.

Es recomendable que el equipo de evaluación investigue información pública y disponible de la organización, en su sitio Web, informes anuales y comunicados de prensa, antes de iniciar la evaluación; con el propósito de comprender mejor la misión empresarial de dicha organización.

5.5.6 Identificación de sistemas críticos

Los sistemas de información identificados en el alcance de la evaluación, deben ser considerados de manera independiente, ya que estos tendrán: activos, funciones, datos, procedimientos, controles y propietarios de datos únicos, además de identificar su criticidad, ya que es un aspecto único.

5.5.6.1. Determinación de la criticidad de los sistemas

El equipo de evaluación debe comprender la importancia de los sistemas críticos para el éxito de la organización, ya que se considera que estos automatizan las funciones críticas del negocio.

La priorización de la criticidad de los sistemas es una tarea difícil, a continuación se describen tres enfoques para determinar esta criticidad:

- *Búsqueda de información adicional*. Es recomendable que aunque ya se tenga información de los sistemas críticos, ésta sea tomada en cuenta para identificar las posibles nuevas amenazas y valorar activos de la organización.
- *Búsqueda de información amplia.* Se recomienda que para identificar la criticidad de un sistema, se recolecte información amplia antes de determinar si el sistema se considera crítico o no.
- *Clasificación de los sistemas críticos*. Para poder identificar los sistemas críticos se recomienda dividir la infraestructura de TI, ya que en muchas organizaciones cuentan con infraestructuras de TI complejas. Es necesario dividir la evaluación en cada unidad de negocio y así tener por separado resultados únicos, prioridades y presupuestos.

5.5.6.1.1. Establecer los requisitos de protección

Los requisitos de protección se derivan de la necesidad de resguardar los elementos de seguridad tales como la confidencialidad, la integridad y la disponibilidad.

La siguiente escala puede ser utilizada con objeto de determinar los requisitos de protección en los sistemas:

- *Protección alta.* Provoca una importante pérdida financiera o requiere de acciones legales para corregir el daño.
- *Protección media.* Provoca una pérdida, no de importancia en las prioridades de la organización o requiere de acciones legales para corregir el daño.
- *Protección baja.* Puede causar pérdidas financieras de poca importancia o sólo requiere de acción administrativa para corregir el daño.

5.5.6.1.2. Precisar los sistemas críticos

La última fase para identificar los sistemas críticos, es precisar cada sistema de información por: aplicación, principales aplicaciones y de soporte general.

- *Aplicación.* Usan la información para satisfacer un conjunto específico de necesidades de los usuarios.
- *Principales aplicaciones*. Requieren una atención especial por el riesgo o daño, en caso de una perdida, mal uso, acceso no autorizado o alteración de la información en la aplicación.
- *Soporte general.* Son un conjunto interconectado de recursos de información con el mismo control de gestión para su funcionalidad.

5.5.7. Identificación de los activos de la organización

Identificar los activos por proteger es un punto clave para la preparación de la evaluación de seguridad, ya que es necesario con objeto de comprender el riesgo total de estos activos.

Identificar los activos que requieren protección puede resultar una tarea fácil si se toma en cuenta la disponibilidad de los controles de seguridad; sin embargo, puede resultar un proceso complicado si se requieren: inventarios, revisión de documentos legales o identificar los activos intangibles, como el prestigio de la organización.

5.5.7.1. Clasificación de la protección de los datos

Los datos de la organización son activos que requieren protección y es prudente clasificarlos, para determinar la protección que requieren y la vulnerabilidad que pudieran tener.

Las organizaciones tiene diferentes razones para proteger sus datos, v.g.: privacidad de los datos personales de los empleados, los datos de propiedad en los precios de los productos, etc. En consecuencia para llevar a cabo la evaluación de seguridad es conveniente determinar si la información es sensible o no, ya que los datos sensibles requieren protección y los datos públicos no. En la tabla 5.1. Se describen los tipos de datos.

CLASIFICACIÓN	DESCRIPCIÓN	EJEMPLOS
DATOS SENSIBLES	Son los datos que contienen información de tipo confidencial, como puede ser la información personal de los empleados, información de configuración de los controles de seguridad y la información de la propiedad de la empresa	Aplicaciones que usan los empleados, contraseñas de las cuentas, etc.
DATOS DEL CLIENTE / INFORMACIÓN DE SALUD PRIVADA	Son los datos que contienen información privada de la salud de los empleados o la información no pública de algún cliente de una entidad financiera	Registros médicos, información de seguro social, estados de cuenta, informes de crédito, etc.
DATOS PÚBLICOS	Es la información que se encuentra publica, por ejemplo, en el sitio Web de la empresa	Sitio Web, información de marketing, etc.

Tabla 5.1. Tipos de datos.

5.5.8. Valoración de activos

La valoración de los activos es un elemento importante para la planificación y contabilidad de la organización. Esta valoración puede ser realizada por diversas razones tales como el cumplimiento de funciones de los activos, la elaboración de presupuestos, la clasificación de información y la determinación de criticidad de éstos.

Podemos identificar cuatro enfoques cualitativos para valorar los activos:

- *Valoración de activos binarios*. Esta valoración se aplica a situaciones en las que se requieren controles específicos de seguridad para activos definidos como muy importantes.
- *Valoración de activos por valor.* Este enfoque agrupa los activos de acuerdo a la importancia que tengan en la organización.
- *Valoración por rango*. Este enfoque valora los activos respecto a los que ya se han identificados y valorados.
- *Valoración por aprobación. D*etermina el valor de los activos a partir de la ayuda y el criterio de un grupo de expertos.

5.5.9. Identificación de amenazas.

El siguiente paso para el equipo de evaluación de seguridad es identificar las amenazas a las que están expuestos los sistemas de la organización, se considera un paso importante ya que limita el daño que se puede ocasionar a la empresa.

5.5.9.1. Elementos de una amenaza.

Una amenaza se describe como un evento con un impacto no deseado sobre los activos de la organización, está compuesta por un agente amenazante y un evento adverso.

- *Agente amenazante*. Es la entidad que puede provocar que la amenaza ocurra, por ejemplo un terremoto.
- *Evento adverso.* Es el evento no deseado inducido por el agente de amenaza y se considera indeseable cuando pone en peligro los bienes de la organización, estos eventos incluyen: daño a las personas, la destrucción de los equipos, la falta de disponibilidad de recursos, etc.

5.5.9.2. Listado de posibles amenazas

Se recomienda que para esta etapa se listen las posibles amenazas a las que está expuesta la organización, en algunas ocasiones esta lista puede haber sido limitada en la fase de definición del proyecto, en donde, por ejemplo, se pueden considerar sólo más amenazas externas

5.5.10. Establecer los controles previstos

En esta etapa, el equipo de evaluación de seguridad debe tener un claro entendimiento de los objetivos de la empresa, los activos a proteger y las amenazas correspondientes a dichos activos. Esta información es necesaria para determinar los requisitos de seguridad y los controles previstos para la organización.

5.6. Recolección de datos para la evaluación.

En cualquier método de evaluación de seguridad la recolección de datos es un punto esencial.

El alcance en la recolección de datos está en función de las siguientes fases:

- *Fase de definición del proyecto*. Define las fronteras del sistema, los controles de seguridad y los activos que se analizarán.
- *Fase de preparación del sistema.* Asegura el tiempo que invierte el equipo para que la recolección de datos sea efectiva y eficiente.

Cuando el equipo de evaluación inicie la recolección de los datos, las definiciones e identificaciones antes vistas, deben haber sido completadas en su totalidad.

5.6.1. Muestreo.

Un muestreo representativo, es la técnica de seleccionar una parte de algo a partir de una población. Si dicha selección aleatoria es realizada correctamente, la prueba es tan precisa como la muestra representativa.

El muestreo es realizado cuando existan constantes de tiempo, presupuesto, situación geográfica u otras que no permitan la prueba completa.

5.6.2. Uso del muestreo en las pruebas de evaluación de seguridad.

El muestreo es una técnica para recolectar una gran cantidad de datos en las pruebas de seguridad, si la muestra es seleccionada correctamente, entonces esta pequeña parte de la población puede proveer la información requerida para la evaluación de seguridad. Se recomienda que el personal encargado de seleccionar dichas muestras conozca los principios básicos del muestreo estadístico.

A continuación se describen dos metodologías para seleccionar una muestra para las pruebas de seguridad:

- *Muestreo representativo*. Una muestra representativa debe contener las características relevantes, en las mismas porciones que la población de la cual se tomó la muestra.

La ventaja de este método es la reducción de costos y datos repetitivos; sin embargo, tiene la desventaja de que en algunos casos los componentes pueden ser diferentes, por lo que deberá cancelarse la muestra.

- *Muestreo seleccionado.* En este método se eligen áreas de la infraestructura que debe ser probada, suponiendo que pueden contener vulnerabilidades.
  Si no es posible probar todas las áreas de la infraestructura o todos los componentes dentro de los sistemas de información, el consultor debe escoger la muestra basándose en su experiencia sobre componentes que pueden contener vulnerabilidades. Por ejemplo, el consultor deberá escoger muestras de las siguientes 30 estaciones de trabajo, tomando en cuenta el caso descrito para el muestreo representativo, esto es:

  - 10 estaciones del departamento de TI.
  - 5 estaciones del departamento. de I&D.
  - 5 estaciones de empleados que trabajan en el turno nocturno.
  - 5 estaciones de mesa de ayuda.
  - 3 estaciones de administradores ejecutivos.
  - 2 estaciones para visitantes.

  Las ventajas de este muestreo incluyen tanto la reducción de costos como la reducción de datos repetitivos, amén de que en la muestra seleccionada es más factible identificar vulnerabilidades que pudieron no ser identificadas a través de otras técnicas y sólo sucedería si la muestra es seleccionada en forma apropiada; Sin embargo también es una desventaja en el caso de que la muestra no sea elegida adecuadamente.

5.7. Recolección de datos físicos.

En la recolección de datos físicos, no considerar las posibles vulnerabilidades físicas puede llevar a un falso sentido de seguridad, e incrementar el riesgo de penetración en activos de información o de capital. Los intentos para penetrar la seguridad de la organización pueden venir de ataques lógicos o físicos, por lo que ignorar el lado físico de la seguridad es una invitación a un desastre.

5.7.1. Amenazas físicas.

Los activos protegidos, en especial los sistemas de computadoras y sus componentes, necesitan ser salvaguardados de condiciones climáticas adversas para asegurar su operación continua. La principal preocupación en aquellas áreas que albergan equipos de cómputo, es el monitoreo y control de las condiciones ambientales, tales como la humedad y la temperatura, así como el suministro de energía eléctrica regulada.

5.7.1.1. Energía eléctrica regulada.

Dado que todos los sistemas críticos dependen de energía eléctrica regulada y de la existencia de transitorios, los siguientes riesgos deben ser considerados:

- *Pérdida de energía.* Muchos factores, incluyendo el clima, sabotaje y fallas del equipo pueden ocasionar pérdida de energía.
- *Suministro de energía con voltaje reducido*. Otros factores, como el clima, las fallas en el equipo o cargas de energía pueden causar caídas momentáneas de voltaje.
- *Suministro de energía con alto voltaje.* Otro tipo de problemas es cuando se entrega un alto voltaje a las instalaciones; esto puede ser causado debido a diversos factores tales como inducciones por relámpagos y fallas en los equipos.

  Acciones preventivas. Las organizaciones deberán considerar las acciones siguientes:

  - *Reguladores de voltaje*. Proveen una salida constante de voltaje, independiente de: la entrada del mismo, la carga de salida o la temperatura.
  - *Supresores de picos*. Este sistema provee protección contra voltajes temporales excesivos.
  - *Acondicionadores de línea*. Estos sistemas regulan, filtran, y suprimen el ruido en fuentes de poder de AC.
  - *Sistemas de fuerza ininterrumpible* (SFI o UPS o No Brake). Estos dispositivos suministran energía eléctrica de respaldo mediante un banco de baterías.
  - *Plantas generadoras de energía eléctrica de emergencia*. Estas son motores a gasolina o diésel, que tienen acoplado un generador de energía eléctrica para proveen energía, en caso de falta del suministro por la compañía encargada de ello y también cuando el tiempo de suministro de baterías se agote posterior a una falla por el suministro.

5.7.1.2. Condiciones ambientales de las salas de cómputo.

Los centros de cómputo al contener equipos que generan calor, deben estas diseñados para regular las condiciones ambientales que se requieran. Para ello, deberá considerarse lo siguiente:

- Alarmas de temperatura.
- HVAC (Heating, Ventilating and Air Conditioning**,** Sistemas de aire acondiconado, ventilación y temperatura).
- Registros de temperatura. Si existen tales registros, estos deben ser revisados 90 días previos a la evaluación.

5.7.1.3 Humedad.

Los ambientes de alta humedad pueden incrementar el riesgo de corrosión en equipos que pueden ser sensibles a ello. La baja humedad incrementa la posibilidad de generación de estática y descargas. Estas pueden dañar o resetear equipos de cómputo sensibles.

Para ello las medidas de seguridad, deben incluir:

- Humidificadores/Deshumidificadores. Es un componente que se instala en el sistema que maneja el aire acondicionado y sirve para añadir o quitar la humedad al aire.
- Alarmas de humedad.
- Registros de humedad. En caso de existir también deben ser revisados, mínimo 90 días previos a la evaluación.

5.7.1.4. Incendio.

El daño provocado por un incendio puede ser limitado o evitado si los controles del edificio son capaces de realizar una detección temprana del fuego, para esto se debe considerar que la organización tenga instalados los siguientes controles:

- Detectores de humo.
- Alarmas contra incendio.

5.7.1.5 Amenazas ocasionadas por el hombre.

En este punto es recomendable realizar un análisis del peligro que el hombre pueda causar a las instalaciones de la organización, ya que pudiera ser ocasionado por el personal que labore dentro o ajeno a ella.

5.7.1.5.1. Revisión al personal.

Se recomienda la revisión al personal antes de que se incorpore a la organización, dicha revisión pueden tomar en cuenta: pruebas de identidad, antecedentes, penales, ciudadanía, referencias, y cumplimiento de obligaciones civiles como el servicio militar.

Se podrán establecer las siguientes medidas físicas:

- *Barreras físicas.* Deben ser usadas para controlar, limitar o excluir el acceso a las instalaciones físicas
- *Puertas.* Con objeto de mejorar la efectividad de las puertas, deberán tomarse en cuenta las siguientes medidas:
  - *Apertura en caso de emergencia*. Este tipo de cierre es esencial para asegurar la seguridad y desalojo del personal en caso de evacuación, la puerta se abre con facilidad al suceder el evento.

- *Apertura facilitada en caso de evento*. Este tipo de cierre, asegura la apertura de los seguros de la puerta, pero no se abre.
- *Cerraduras.* El tipo y efectividad de las cerraduras dependerán de la información o área que se desee proteger.

5.7.1.6. Alumbrado de las instalaciones.

El alumbrado es un control de seguridad físico, esencial para prevenir accesos no autorizados que pudieran poner en peligro al personal. Además incrementa la vigilancia al iluminar los linderos de las propiedades, tales como entradas, salidas y otras áreas críticas.

5.7.1.7. Detección de intrusos.

Los sistemas de detección de intrusos también conocidos como sistemas de seguridad electrónica, deben estar implementados para detectar, retrasar y responder a las actividades de intrusos. Personas que no tengan autorización de acceso a los sistemas, son peligro para la seguridad y un riesgo para los activos de la organización.

Es recomendable revisar los siguientes controles:

- Controles físicos de acceso. Tales como barreras perimetrales, o cerraduras adicionales.
- Prevención de entradas no autorizadas.
- Métodos de identificación. Tales como alguno(s) de los siguientes: lectores de tarjetas, sistemas de credenciales, digitación de claves con contraseñas, controles biométricos, etc.

5.7.2. Uso del método RIIOT (Review, Interview, Inspect, Observe and Test) para la recolección de los datos físicos.

Cabe mencionar que una introducción a este método RIIOT se refirió al final del capítulo 2; por ahora lo trataremos de la siguiente manera:

- *Revisión de los documentos físicos.* Para tener una perspectiva de la situación real de la empresa se recomienda la revisión de toda la información de seguridad disponible; por ejemplo: manuales, especificaciones, normas, procedimientos, registros, etc. Conviene considerar los registros que se tuvieren de evaluaciones anteriores, con objeto de utilizar la información recolectada y así mejorar los resultados por obtener.
- *Entrevistas al personal clave*. En estas entrevistas debe incluirse al encargado de las instalaciones, miembros del equipo de seguridad y personas involucrados en la selección, operación o mantenimiento de los controles físicos de seguridad. Al finalizar las entrevistas, se podrá obtener un entendimiento detallado de las medidas de seguridad empleadas en el sitio.

- *Inspección de los controles.* Durante esta etapa se revisarán los controles de seguridad establecidos y la información recolectada deberá ser confirmada en este proceso de inspección, a través de la revisión física y las evidencias obtenidas, tales como las bitácoras de entradas y salidas de personal, las bases de datos, reportes y archivos de auditoría que cubran el área y el tiempo especificado en el alcance.
- *Observación del comportamiento del personal*. Este proceso es pasivo y revisa el conocimiento y la forma de trabajar del personal, con relación a los procedimientos implementados.
- *Probar los controles.* Finalmente, probar los controles de seguridad es generar las condiciones que activen las protecciones físicas respecto a los controles de seguridad establecidos.

Existen numerosas amenazas a la seguridad física, algunas de estas, las más frecuentes, se comentan en la tabla 5.2. En este inciso 5.7. Recolección de datos físicos, se han descrito las amenazas generales de seguridad física y contramedidas, así como un proceso de información en cuanto a la adecuación de los mecanismos de seguridad física.

ÁREAS FÍSICAS Y AMENAZAS	TIPO	ECHOS	CONTRAMEDIDA(S)
Infraestructura, (oficinas, almacenes, talleres, etc.) Condiciones ambientales	Potencia o energía eléctrica	Potencia inconsistente	Supresor de sobrevoltaje
		Sin alimentación de potencia	Transmisor de energía (Transfer)
			Sistema de fuerza ininterrumpible
			Planta para generación de energía eléctrica
	Calefacción	Refrigeración no disponible	Ventilación, calefacción y aire acondicionado
		Refrigeración insuficiente	Alarma de temperatura
			Registro de temperatura
	Humedad	Altos niveles de humedad	Humidificador/deshumidificador
		Bajos niveles de humedad	Alarma de humedad
			Registro de humedad
Incendio	Exposición al fuego	Daños a personas	Construcción de edificios
		Daño a los activos	Detalles de la construcción
			Almacenamiento de combustibles
			Salidas de emergencia
			Evacuación por incendio

	Detección de incendios	Daño a personas	Detectores de humo
		Daños a los activos	Detectores de calor
			Detectores de humo
			Ubicación del detector de incendios
	Alarma de incendios	Daño a personas	Paneles de control
		Daños a los activos	Alarmas audibles
			Alarma visibles
			Alarmas auxiliar
			Estación central
			Estaciones remotas
	Extinción de incendios	Daños a personas	Gas inerte
		Daño a los activos	Gas inerte, agua
			Espuma
			Arena limpia
Inundación	Daños por inundación	Daños a personas	Desagüe libre de obstáculos
		Daño a los activos	Bolsas de arena para proteger entradas
	Exponerse a la inundación	Daños a personas	Bombas de agua para extracción
		Daño a los activos	Pisos elevados seguros
Otros desastres naturales	Exposición a elementos naturales	Daños a personas	Protección por inducción eléctrica (Jaula de Faraday)
		Daño a los activos	Alarma sísmica
			Semáforo de alerta volcánica
			Cortinas anticiclónicas
Protección del empleo	Revisiones al personal	Confianza alterada	Prueba de identificación
		Problemas Legales	Verificación de antecedentes
			Pruebas de ciudadanía
			Acreditación de servicio militar
Protección de instalaciones	Barreras o muros de protección o puertas de seguridad	Entrada no autorizadas	Cercar las instalaciones
		Poner en peligro a los empleados	Edificios seguros
			Puertas seguras
			Cerraduras seguras
			Barreras vehiculares

	Alumbrado	Poner en peligro a los empleados	Alumbrado fijo
			Alumbrado en espera
			Alumbrado móvil
			Alumbrado de emergencia
	Detección de intrusos	Entrada no autorizada	Sensores de movimiento
			Mantener un registro de personas Videocámaras de seguridad
		Poner en peligro a los empleados	Sensores internos de movimiento
			Circuito cerrado de televisión
	Activos físicos	Entrada no Autorizada de objetos	Prohibir el acceso de objetos extraños
		Extracción no autorizada de la propiedad	Personal de vigilancia 7x24
			Inspección de paquetes extraños
			Control de entrada y salida de materiales (consumibles, elementos desechables)

Tabla 5.2. Amenazas y contramedidas físicas.

5.8. Recolección de datos técnicos

En la recolección de datos técnicos, las amenazas técnicas son el punto de análisis para esta parte de la evaluación, es recomendable que el equipo de seguridad tenga un claro entendimiento de las amenazas y la protección del área técnica de seguridad.

5.8.1. Control de la información

La información es uno de los activos más valiosos de la organización, por lo que se recomienda el implementar controles de seguridad técnicos adecuados y así asegurar que la información sensible está protegida.

5.8.1.1. Error del usuario.

Los controles de protección se utilizan para evitar fraudes, abusos y ataques; sin embargo, aun con buenas intenciones, eventualmente los empleados pueden violar la seguridad de la organización a través de situaciones accidentales, a esto se le llama errores del usuario.

Los controles técnicos que se mencionan a continuación son algunas de las formas de minimizar los errores del usuario:

- *Tecnología de monitoreo.* Incluye cualquier dispositivo técnico o aplicación que pueda monitorear el comportamiento de un usuario en el sistema. Por ejemplo, el seguimiento del URL (Universal Resource Locator) puede informar sobre los hábitos de los usuarios navegando en Internet o incluso bloquear este tipo de comportamiento, además de monitorear o bloquear la información recibida o enviada vía correo electrónico.
- *Registros de auditoría.* Contienen los datos registrados por el sistema en eventos relevantes para la seguridad. Los datos contenidos en estos registros deberán incluir como mínimo la siguiente información: identificación, hora, evento y el éxito o fracaso de éste.

5.8.2. Información sensible y crítica.

Para la organización toda la información es valiosa, algunos datos son más críticos y sensibles que otros, por ello es recomendable implementar controles técnicos de seguridad a fin de protegerlos contra su divulgación o modificación y asegurar su disponibilidad.

- *Controles de acceso lógico.* Este tipo de controles son implementados para acceder a los archivos críticos y sensibles, basándose en la identidad del usuario y los controles implementados en los archivos.
- Checksums. Las sumas de comprobación criptográficas proporcionan un método para la detección de modificaciones no autorizadas a los archivos confidenciales. La integridad del archivo es determinada calculando nuevamente el valor numérico y comparándolo con el valor almacenado. Si los valores no coinciden, la integridad del archivo ha sido comprometida.
- *Encriptación.* El cifrado es la conversión de un texto en forma irreconocible; sin embargo, el término cifrado, generalmente se utiliza para describir la aplicación de una o más técnicas que se usan para garantizar la confidencialidad, integridad y autenticidad de información sensible y critica.
- *Sistemas Anti-Virus.* Componentes esenciales de los controles técnicos de seguridad, ya que son necesarios por lo robusto que pueden llegar a ser los sistemas en una organización y la amenaza constate de ataques de código malicioso.

5.8.3. Continuidad del negocio

La continuidad del negocio es la parte de la preparación y la planificación llevada a cabo por las organizaciones con objeto de asegurar que son una entidad viable, aun cuando un desastre afecte a sus sistemas críticos.

5.8.3.1. Planes de contingencia.

Los planes de contingencia implican un análisis de los posibles riesgos a los cuales pueden estar expuestos el personal, los equipos de cómputo y la información contenida en los diversos medios de almacenamiento, por lo que en dichos planes se debe considerar un estudio de los riesgos, la forma de reducir su posibilidad de ocurrencia y los procedimientos a seguir en caso que se presentara el problema.

Pese a todas nuestras medidas de seguridad puede ocurrir un desastre, por tanto, es necesario que los procedimientos o planes de contingencia incluyan un *plan de recuperación de desastres*, el cual tendrá como objetivo restaurar el servicio de cómputo en forma rápida, eficiente y con el menor costo y pérdidas posibles.

- *Copia de seguridad de datos.* Los datos críticos deben ser respaldados para asegurar su disponibilidad inmediata posterior al desastre. Dependiendo del objetivo de la recuperación de los datos, existen diferentes tecnologías para los respaldos mediante una o varias copias de seguridad, mismas que deberá resguardarse dentro y fuera del edificio que alberge al centro de cómputo.
- *Conjunto redundante de discos independientes.* La matriz redundante de discos independientes (Redundant Array of Independent Disks, RAID) es una tecnología utilizada para la redundancia y la mejora del rendimiento. Esta tecnología combina varios discos físicos y los integra en una matriz lógica. Existen varios tipos de RAID que proporcionan diferentes niveles de mejoras en el rendimiento y redundancia.

5.8.4. Arquitectura segura

La seguridad de un sistema de información depende de la estructura y los servicios proporcionados por la arquitectura bajo la cual se opere; debido a la falta de una buena estructura, la seguridad se limita y puede permitir el acceso de ataques vía red, espionaje , etc.

Aspectos claves de la arquitectura de un sistema seguro.

- *Topología.* Una topología de red es la disposición física y lógica de sus componentes. La protección que puede tener se describe a continuación:
  - *Defensa en profundidad*. Establece que los activos críticos no sólo deben tener mecanismos únicos para su protección, sino que sus enfoques de defensa serán diferentes.
  - *Segmentación de la red*. Es un subconjunto de una red delimitada por dispositivos tales como ruteadores, switches, puentes, entre otras. Al dividir una red en segmentos obtiene rendimiento y seguridad debido a la limitación del tráfico.

- *Seguridad en los dominios.* Es una agrupación lógica de las computadoras en una red en la que existe una relación de confianza entre todas las estaciones de trabajo.
- *Redundancia.* Es la protección cuando se tienen procesos idénticos trabajando, en caso de que uno falle, se cuenta con un respaldo constante y el trabajo no no se interrumpe.

5.8.5. Uso del método RIIOT (Review, Interview, Inspect, Observe and Test) para la recolección de datos técnicos.

La aplicación del método RIIOT al área técnica incluye cinco puntos.

- *Revisión de documentos técnicos.* Consiste en la revisión de documentos de los controles de seguridad técnicos, los cuales la mayor parte serán manuales y diagramas, el resto de las revisiones incluirán los mapas de red y declaraciones de políticas técnicas, entre otros.
- *Entrevista al personal técnico.* Consiste en entrevistar al personal técnico para entender los controles técnicos empleados, así como la estructura de la red, etc. Dentro del área de controles técnicos, el equipo de seguridad tomará las entrevistas como información complementaria, siendo las pruebas e inspecciones la principal fuente de información.
- *Inspección de los controles de seguridad técnicos.* La inspección consiste en la revisión de los aspectos de los controles de seguridad, por ejemplo las configuraciones o arreglos; así mismo, de la información recopilada, se verifica la identificación de vulnerabilidades y se documentan los resultados.
- *Observar el comportamiento del personal técnico.* El proceso de recopilación de datos a través de la observación del comportamiento del personal técnico debe ser sutil, ya que este proceso es pasivo y depende del personal técnico; el ser consistentes con las políticas de la organización, los procedimientos, el mantenimiento y el uso correcto de la tecnología determina la eficacia de los controles técnicos.
- *Prueba de los controles técnicos de seguridad.* Es el proceso de poner a prueba los controles técnicos de acuerdo a las funciones de seguridad previstas. Estas pruebas permiten tener una excelente visión de la eficacia de dichos controles. Los controles técnicos aptos para estas pruebas incluyen: los registros de auditoría, sistemas anti-virus, directivas automatizadas de contraseñas, VPN (Virtual private network**)** , Firewall (cortafuegos), IDS (Intrusion detection system**)**, entre otros.

Un miembro del equipo de evaluación de seguridad es eficaz, cuando tiene una comprensión básica de las amenazas y contramedidas dentro del área de seguridad técnica, algunas de las amenazas más frecuentes se analizan en la siguiente tabla 5.3.

Las amenazas técnicas incluyen la divulgación, modificación, denegación de servicio y otras amenazas que afectan a los activos de la organización.

Las contramedidas técnicas son controles lógicos que pueden reducir estas amenazas a través de la prevención, detección o corrección.En este inciso 5.8. Recolección de datos técnicos, en la tabla 5.3., se han descrito las amenazas generales de seguridad técnica y sus contramedidas, así como un proceso de información en cuanto a la adecuación de los mecanismos de seguridad técnica.

ÁREAS TÉCNICAS Y AMENAZAS	TIPO	ECHOS	CONTRAMEDIDA(S)
Control de información	Error del usuario	Ingeniería social	Definir una política de seguridad
		Errores involuntarios	Registros de auditoría
			No instalar programas sin autorización Tecnologías de monitoreo
	Información sensible / critica	Divulgación	Controles de acceso a los equipos (privilegios de acceso)
		Modificación	Listas de comprobación
			Cifrado de datos
			Sistema antivirus
	Cuentas de usuario	Divulgación	No compartir contraseñas
		Modificación	Política de contraseña robusta
			Realización de mantenimiento preventivo (protección de identidad)
Continuidad del negocio	Planes de contingencia	Divulgación	Tecnologías de respaldo para seguridad de datos
		Falta de disponibilidad	RAID
	Programa de respuesta a incidentes	Divulgación	La estrategia de continuidad del negocio
		Desestabilización	
		Fraudes	Análisis del impacto comercial
			Plan de recuperación de Desastres (DRP)
			Pruebas de DRP y mantenimiento
			Plan y procedimientos de respuesta a incidentes
			Capacitación de respuesta a incidentes
Seguridad del sistema	Controles de acceso y aplicaciones de seguridad	Divulgación	Controles de acceso lógico
		Desestabilización	Herramientas de rastreo de vulnerabilidades
		Fraudes	
		Ataques al sistema	Eliminar servicios innecesarios
		Falta de disponibilidad	Sistema de Detección de Intrusos (IDS)
			Anti-virus y anti-spam

			Eliminación de software espía
			Actualización constante del software instalado
			Firewall de nivel de aplicación
			Firewall de nivel de sesión
			Bloquear documentos adjuntos sospechosos
			Análisis y evaluación de riesgos
			Parches programados y de emergencia
			Revisión de seguridad/autorización
			Normas de codificación
			Revisión de código
			Requisitos de seguridad mínima
			Revisión de la seguridad a terceros
			Mantenimiento a distancia
Arquitectura	Topología de red	Defectos de diseño	Protocolos seguros
		Ataques a la red	Segmentación de la red
			Seguridad en los dominios
			Redundancia
			Evaluación de productos
		Espionaje	Cifrado de comunicaciones y datos
			Seguridad del tráfico en la red
			Aislar las amenazas
Datos	Almacenamiento	Divulgación	Cifrado de archivos
		Modificación	Auditor código
	Transito	Divulgación	Cifrado de red
		Modificación	Red privada virtual Cifrado de correo electrónico

Tabla 5.3. Amenazas y contramedidas técnicas

5.9. Recolección de datos administrativos

Las amenazas administrativas son el principal punto para la recopilación de datos administrativos, las más frecuentes se describen a continuación.

5.9.1. Recursos Humanos

Es importante que las organizaciones protejan sus activos del personal no calificado o poco fiable, dicho personal a través de actos accidentales o intencionales puede exponer los activos a la divulgación, integridad y disponibilidad ajena, por lo que es recomendable establecer controles de seguridad durante la estancia de un empleado.

- *Reclutamiento.* Es importante que el departamento de Recursos Humanos antes de contratar a un empleado, cuente con exigentes procedimientos de contratación y controles de seguridad que garanticen la confiabilidad del empleado, con ello tratar de evitar el error o abuso del personal.
- *Contratación.* Una vez que un individuo se convierte en empleado, la posibilidad de cometer algún error, fraude o abuso, puede afectar la seguridad de los activos de la organización, por lo que es recomendable tener varios enfoques para proteger los activos en caso de amenazas potenciales.
- *Terminación del contrato.* Los procedimientos de terminación de un contrato deben ser tratados de manera delicada para evitar una brecha en la seguridad, ya que empleados no conformes que han tenido acceso a la información sensible y a los sistemas críticos pueden cometer abusos o fraudes.

5.9.2. Estructura organizacional

La estructura de la organización tiene un papel importante en la aplicación efectiva de los controles de seguridad; un mal manejo en la organización de los servicios, las responsabilidades y las estructuras de la información pueden afectar los controles de seguridad básicos.
La importancia que tiene la estructura organizacional, de acuerdo con los controles de seguridad administrativos, es la siguiente.

- *Alta dirección.* Toda seguridad comienza en la parte superior, por lo que esta es la última instancia responsable de la seguridad y está encargada de informar los resultados a los propietarios. La alta dirección también establece la estructura organizacional y la funcionalidad de los controles de seguridad.
- *Programa de seguridad.* Es el responsable de la supervisión, la gestión y dirección de los controles de seguridad dentro de la organización. Un programa de seguridad bien estructurado, con personal y buen financiamiento ofrecer muchas ventajas de seguridad.
- *Operaciones de seguridad*. Este equipo es el responsable de la implementación y mantenimiento de controles de seguridad técnicos, su tarea es administrar dichos controles, firewalls y software anti-virus.
- *Auditoria.* Su función es supervisar las tareas y la protección de los activos sensibles de la organización, así como la auditoría interna y evaluaciones de riesgos de seguridad.

5.9.3. Control de información

La información es uno de los activos más valiosos de la organización, por lo que es importante implementar controles de seguridad adecuados para proteger la información sensible.

Se sugiere aplicar controles de seguridad para los siguientes enfoques.

- *Cuentas de usuario.* Contiene los datos del usuario tales como: su nombre, área o departamento al que pertenece, privilegios autorizados, fechas de inicio y expiración de permisos y accesos. Considerando los tipos de privilegios es posible que tenga acceso a los recursos y archivos críticos de la organización, por lo que debe ser estrictamente vigilado.
- *Error del usuario.* Es posible que accidentalmente los empleados puedan violar la seguridad de la información, por lo que se sugiere implementar controles administrativos con el fin de limitar los posibles errores del usuario.
- *Control de activos.* Implica el control y seguimiento de todos y cada uno de los activos de la organización, ya sean los activos tangibles e intangibles.
- *Información sensible.* Toda la información es valiosa, pero algunos datos son más críticos y sensibles que otros, por ello la organización debe identificar esta información y proporcionar controles adicionales para proteger su divulgación.

5.9.4. Seguridad del sistema

Es recomendable que la organización proteja sus sistemas de información de los cambios no programados, por ejemplo el acceso de terceros, las vulnerabilidades a nivel de sistema y a nivel de aplicación; cualquiera de estas amenazas podría conducir a la divulgación o que se corrompiera la información sensible, e incluso llegar al fraude; por lo que deberemos estar pendientes de los siguientes aspectos:

- *Controles del sistema.* Protegen de las posibles aplicaciones falsas y de usuarios no autorizados, incluyen políticas, procedimientos y actividades de seguridad que descubren, reducen y evitan las vulnerabilidades en los sistemas de información.
- *Seguridad en las aplicaciones*. Es recomendable implementar controles de seguridad a las aplicaciones Web, a pesar de que están protegidas por firewall y el sistemas operativos, están expuestas a tener errores y ser vulnerables.
- *Gestión de la configuración.* Es el proceso de identificar las variables de configuración de los equipos, por ejemplo; el nivel de almacenamiento, cambios en la configuración del sistema, entre otros.

5.9.5. Uso del método RIIOT (Review, Interview, Inspect, Observe and Test) para la recolección de los datos administrativos.

Para la recolección de datos administrativos, el método RIIOT, se aplica de la siguiente manera:

- *Revisión de los documentos administrativos.* Los elementos que son prioridad para ser revisados son las políticas y procedimientos, enseguida se revisan las políticas de seguridad de la información, los cursos para concientizar a los empleados respecto a la seguridad y los documentos que generen las actividades de seguridad. Todos los documentos revisados deben ser claros, concisos y completos.
- *Entrevistar al personal administrativo*. Es importante que el personal del equipo de evaluación determine la información que requiere y así entrevistar al personal indicado, las preguntas corresponderán únicamente a lo que se requiere.

  Considérense los siguientes puntos en el proceso de entrevistas:
  - Dar prioridad a preguntas concretas referentes a controles de seguridad clave.
  - Obtener opiniones de diferentes perfiles sobre un mismo tópico.
  - Preguntar por los pasos que se siguieron en algún evento reciente y compararlo con lo que está descrito en las políticas y procedimientos.

- *Inspeccionar los controles de seguridad administrativos.* Respecto a que la inspección es diferente a la prueba, en el sentido de que la inspección es realizada cuando la prueba es inapropiada o no factible. La inspección requiere de la revisión de los controles de seguridad y de aspectos como las configuraciones de los equipos; principalmente se revisan los controles de seguridad, la información recolectada, las vulnerabilidades encontradas y la documentación de los resultados.
- *Observar el comportamiento del personal administrativo*. Normalmente este proceso es pasivo y depende de que los miembros del equipo conozcan las políticas y procedimientos, así como también puedan confirmar o desaprobar el apego de la organización a sus propias políticas y procedimientos.
- *Probar los controles administrativos.* En este punto se generan condiciones que activen los controles administrativos y de esta forma poner a prueba la respuesta a las políticas, procedimientos y las buenas prácticas. Este tipo de recolección de datos proporciona una visión amplia de la efectividad de los controles.

Es indispensable que uno o varios miembros del equipo de evaluación de seguridad tengan un conocimiento básico de las amenazas y contramedidas dentro del área de seguridad administrativa, algunas de las amenazas más frecuentes se analizan en la siguiente tabla 5.4.

Las amenazas administrativas incluyen: errores, omisiones, fraudes, despilfarro, abuso, negligencia, privilegios excesivos y otras amenazas que afectan a los activos de la organización. Las contramedidas administrativas son las políticas, los procedimientos y las actividades que pueden reducir estas amenazas.

ÁREAS FÍSICAS Y AMENAZAS	TIPO	ECHOS	CONTRAMEDIDA(S)
Recursos humanos	Personal de poca confianza	Errores del personal	Definir políticas de seguridad
		Intercepción de información	Definir responsabilidades
			Verificación de referencias
		Fraudes	Aplicar el plan de contingencias
		Abusos	Terminación del contrato
	Personal no calificado	Uso incorrecto de aplicaciones	Aplicar políticas de empleo
			Educación comprobable
		Falta de concientización	Capacitación de empleados y usuarios
			Requisito de experiencia
		Abusos Fraudes	Monitoreo constante
			Formación ética
			Políticas de sanciones
Estructura de la organización	Personal	Fraude	Separación del trabajo
		Ineficacia	Auditoria interna
		Abuso	Procedimientos de terminación de contrato
			Exámenes de conocimientos
			Capacitación continua
	Alta dirección	Negligencia	Auditoria
		Fraudes	Separación de funciones
		Abusos	Asignación de deberes
			Menos privilegios
Control de información	Información sensible	Divulgación	Políticas y procedimientos
		Uso incorrecto	Monitoreo
		Robo	Análisis de criticidad de información
			Revisión de los controles de acceso
			Destrucción de medios de almacenamiento
			Destrucción de documentos
	Cuentas de usuario	Divulgación	Procedimientos de creación de la cuenta
		Privilegios excesivos	Revisión de los controles de acceso
		Robo	Procedimientos de terminación de la cuenta
			Políticas de contraseña robusta
			Cambios de contraseña frecuentemente

Tabla 5.4. Amenazas y contramedidas administrativas.

5.10. Análisis de los riesgos de seguridad

La siguiente fase de una evaluación es el análisis de los riesgos de seguridad. Este análisis depende de que las etapas de recolección de información, entreguen la información requerida para analizar los riesgos de seguridad. El proceso para evaluar los riesgos de seguridad se resume en los siguientes tres pasos:

- Determinar el riesgo de seguridad.
- Generar los riesgos de seguridad, a manera de sentencias o enunciados.
- Revisión de las sentencias o enunciados por el equipo de seguridad.

5.10.1. Determinar el riesgo de seguridad

El objetivo primordial del proceso de evaluación de seguridad es determinar los riesgos que afectan a los activos de la organización, por medio de la identificación de amenazas y vulnerabilidades, basándose en la probabilidad y el impacto de la dupla amenaza/vulnerabilidad.

Con los datos que se obtiene en la fase de recolección de datos, el cálculo de los riesgos de seguridad puede ser realizado.

La ecuación básica para el cálculo de estos riesgos es la siguiente:

Riesgo = Activos X Amenazas X Vulnerabilidad

Para calcular esta fórmula, se considera que ya se ha evaluado el valor del activo, el tamaño de la amenaza y la posibilidad de que la amenaza sea explotada a través de una vulnerabilidad existente.

Sin embargo, esta sencilla ecuación es solamente el principio del cálculo del riesgo de seguridad, ya que los diferentes métodos de evaluación tienen en particular su forma de especificar las variables e interpretar los resultados.

Es importante mencionar que el propósito de la metodología propuesta, es preparar a las personas y equipos para que participen efectivamente en cualquier esfuerzo de evaluación de riesgos de seguridad.

5.10.2. Determinar los puntos claves de riesgos de seguridad.

Un punto clave de riesgo de seguridad, es una forma de presentar la información encontrada en un enunciado de riesgo de seguridad. Debido a que entre las evaluaciones de los activos, la frecuencia de las amenazas y los posibles daños; hay muchos valores o números a los cuales se les debe dar seguimiento, por lo que es recomendable determinar dichos puntos.

A continuación se presenta la Tabla 5.5. con tres ejemplos de puntos claves de riesgos de seguridad:

Amenaza	Vulnerabilidad	Objetivo de la vulnerabilidad	Política violada	Activo expuesto
Un competidor	Uso de la ingeniería social	Oficinas de venta	Revelar información interna	Lista de activos clave
Un hacker	Explotación de vulnerabilidades conocidas	En algún protocolo de autenticación remoto	Ingresar sin autorización	Autenticación remota de servidores
Un intruso	Puede introducirse sin autorización	Al site de telefonía	Espiar conversaciones telefónicas	Conversaciones confidenciales

Tabla 5.5. Ejemplos de los puntos claves de riesgos de seguridad.

Este simple conjunto de enunciados de riesgos de seguridad es útil en evaluaciones a pequeña escala, cuando no hay necesidad de establecer una gran cantidad de enunciados de riesgos de seguridad.

5.10.3. Revisión de los puntos claves de riesgo de seguridad por el equipo de seguridad.

Tomando en cuenta que generalmente se obtiene una gran cantidad de información durante las etapas de recolección de datos, es óptimo para el equipo de evaluación dividirse las tareas para crear los puntos clave de riesgos de seguridad. Generalmente, estos pueden dividirse en las diferentes áreas de estudio, tales como la administrativa, la física y la técnica. Posteriormente pueden dividirse las áreas técnicas, de acuerdo a los sistemas o subgrupos de sistemas.

Los miembros del equipo deberán trabajar solos o en pequeños grupos (por ejemplo, de dos personas) para crear los puntos clave de los riesgos de seguridad que cubran los datos que tengan asignados. Una vez que se tiene el borrador de puntos clave completo, el líder del equipo deberá reunir la lista completa y distribuir copias a todos los miembros, para que la siguiente tarea de todo el equipo sea revisar dicho borrador y llegar a un consenso de los puntos y los valores de los datos contenidos en estos.

5.10.4. Establecer los riesgos de seguridad para la organización.

Finalmente, el equipo de evaluación debe establecer un riesgo de seguridad global, esta medición deberá ser consistente con los alcances del proyecto y los rangos usados para describir los riesgos de seguridad individuales.
En general, el riesgo de seguridad global deberá indicar un riesgo de seguridad relativo, como por ejemplo: *Riesgo de seguridad moderado* y una comparación que establezca en donde se encuentra la organización con respecto a otras del mismo ramo.

Los detalles técnicos de las mediciones no se necesitan listar, ya que el objetivo es que la alta dirección conozca la tolerancia que tiene la organización respecto a los riesgos de seguridad encontrados.

5.11. Mitigación de los riesgos de seguridad

Las recomendaciones que se hacen en esta fase son conocidas como *contramedidas*, las cuales son implementadas con la intención de reducir los riesgos de seguridad encontrados. A continuación se mencionan algunos de los métodos más utilizados en donde se implementan estas contramedidas:

5.11.1. *Método 1.* La falta de controles indican la necesidad de contramedidas.

La implementación de contramedidas para mitigar un riesgo o vulnerabilidad se lleva a cabo debido a una amenaza o vulnerabilidad detectada. Por ejemplo, si una organización no tiene documentado un plan de respuesta a incidentes, la contramedida será el crear dicho plan, aunque esto parezca simple, la mejor manera de tratar un riesgo expuesto, es eliminarlo.

5.11.2. *Método 2.* Personal, procesos y tecnología.

Este método se enfoca en las posibles contramedidas aplicadas al personal, procesos y diversas tecnológicas.
Para el personal; se deben considerar contramedidas enfocadas al mismo; en el caso de los procesos, el equipo de evaluación debe considerar contramedidas de acuerdo a los procesos; tales como programas de concientización de seguridad y revisión de perfiles, entre otras. Y finalmente las contramedidas tecnológicas se basan en la autentificación de dos factores: los sistemas de detección de intrusos y el filtrado de correo no deseado.

5.11.3. *Método 3.* Administración y aspectos técnicos.

Similar al método anterior, este considera las categorías de contramedidas expuestas en los temas de recopilación de información, que se mencionan en este capítulo.

5.11.4. *Método 4.* Prevención, detección y corrección.

Este método se enfoca en el resultado deseado por la contramedida, ya que en primer lugar procura prevenir que sucedan los incidentes y detectar cuando acontecen, además de corregir los incidentes, una vez que ocurren. Por ejemplo, un sistema antivirus está diseñado para prevenir que los virus infecten a la computadora, detectar cuando ingresan al sistema y además erradicarlos una vez que se detectan.

5.11.5. *Método 5.* Tecnología disponible.

Es importante que el equipo de evaluación se capacite constantemente en las nuevas tecnologías de seguridad, a través de seminarios, literatura e implementaciones recientes, las cuales serán de utilidad para emplearse en las recomendaciones de mitigación de riesgos que sean necesarias para la empresa.

5.12. Recomendaciones para el reporte final.

Uno de los elementos más importantes en la evaluación de seguridad es la comunicación clara y eficaz de los resultados, por lo que se recomienda que el reporte final contenga información precisa, no amenazante, relevante e inequívoca.
Recordando que el objetivo de la evaluación de seguridad, es proporcionar información a la alta dirección para apoyar las decisiones de implementar contramedidas o aceptar los riesgos en los activos de la organización; a continuación se presentan algunos aspectos importantes por considerar en el reporte final.

5.12.1. Precaución en el informe.

El equipo de evaluación de riesgos de seguridad debe tener cuidado en el informe no solamente en lo que dice, sino cómo lo dice. El siguiente análisis pretende ofrecer algunas sugerencias sobre la elaboración del informe de resultados.

- *Evitar señalar culpables.* El equipo de evaluación de riesgos de seguridad debe evitar declaraciones que puedan interpretarse como el señalar culpables culpas.
- *Evitar retrasos en la presentación del informe*. Es importante que el informe se entregue en el tiempo acordado, ya que muchas de las observaciones, conclusiones y recomendaciones, están en funcionamiento y es esencial que se actué oportunamente, antes de que suceda un incidente. También es recomendable que exista una revisión inicial con el cliente, para asegurar la precisión y la finalización de los objetivos entregables.
- *Incluir los resultados positivos.* El informe de evaluación de riesgos de seguridad es una herramienta muy importante para la alta dirección de la organización. Sin embargo, al igual que un informe de auditoría, está conformado con una lista de las muchas áreas de mejora, por lo que se recomienda que el informe tenga un enfoque positivo, dando a entender que con el tiempo se pueden implementar muchas de las recomendaciones.

5.12.2. Estructura del informe.

Una adecuada estructura del informe, mejora en gran medida su legibilidad y facilidad de uso. Debido a que el informe está diseñado para diferentes públicos, por lo que debe contener secciones para cada tipo de audiencia, que pueden ser tanto directivos como administradores y ejecutivos de recursos técnicos.

5.12.2.1. Nivel ejecutivo del informe

El informe ejecutivo está diseñado para la alta dirección de la organización, esta sección contiene la información que es necesaria para la toma de decisiones. Se sugiere considerar las siguientes recomendaciones para dicho informe.

- *Longitud.* El informe ejecutivo debe considerar un máximo de dos a cuatro cuartillas.
- *Elementos clave.* Describen el propósito de la evaluación, el enfoque de la evaluación, las principales conclusiones, recomendaciones y pasos a seguir.
- *Buenas recomendaciones.* Los ejecutivos toman las decisiones con base a las recomendaciones y la información disponible, se recomienda que el equipo de evaluación como experto, proporcione sugerencias claras y precisas.
- *Detalles técnicos.* El resumen no debe contener información técnica detallada, sin embargo debe estructurarse de forma tal que la búsqueda de detalles sobre los hallazgos y recomendaciones sea ágil.

5.12.2.2. Información base.

El informe debe proporcionar la mayor parte de la información recopilada durante el proceso de evaluación. La estructura del informe puede ser establecida en la definición del proyecto, de no ser así se recomienda tomar como base la siguiente estructura.

- *Introducción.* En esta sección se ofrece una introducción a la evaluación de riesgos de seguridad, debe contener la información necesaria para que alguien ajeno a la evaluación, pueda entender en qué consiste el proyecto
- *Características del sitio.* Describe las contramedidas físicas existentes, los factores ambientales y la ubicación geográfica de los sistemas de información a ser evaluados; se recomienda incluir la instalación de controles de acceso, zonas restringidas, fuentes de energía, características de seguridad y sistemas ambientales.
- *Características de los sistemas de información.* Describe las medidas de seguridad técnicas existentes, se recomienda incluir: la clasificación de los datos, la protección contra virus, software de copias de seguridad, sistemas de identificación y autenticación, además de todos los otros controles técnicos.
- *Características organizacionales.* Describen las medidas de seguridad administrativas existentes, se recomienda incluir políticas, procedimientos y actividades de seguridad que actualmente realiza el personal de la organización o subcontratados. Un organigrama que destaque la organización de la seguridad también debe ser incluido y discutido.
- *Análisis de activos y amenazas* .Incluir un informe sobre el análisis de activos y las posibles amenazas a la organización.
- *Análisis de la vulnerabilidad*. Incluir un informe sobre las vulnerabilidades identificadas.
- *Análisis de riesgos de seguridad*. Incluir los resultados de los análisis de riesgos de seguridad.
- *Recomendaciones de medidas de prevención*. Enlistar las medidas recomendadas.

5.12.3. Informe provisional

La elaboración de un informe provisional de la evaluación de riesgos de la seguridad es esencial para el éxito del proyecto. Un proyecto de informe proporciona dos funciones importantes:

- *Regeneración inmediata.* El informe provisional de evaluación de riesgos de seguridad proporciona una retroalimentación inmediata al cliente para las brechas de seguridad de alto riesgo. Si el equipo de evaluación ha descubierto y documentado las brechas de seguridad de alto riesgo que se deben abordar de inmediato, el proyecto de informe es un vehículo útil para dejar una constancia y recomendaciones documentadas para abordar estas áreas. Por ejemplo, un proyecto de informe podría contener los resultados de los análisis y recomendaciones para los parches de vulnerabilidad.
- *Oportunidad para la corrección*. En el curso de la revisión de documentos, la realización de entrevistas, inspección de los controles, la observación de la conducta y la prueba de los controles, los errores serán hechos por el equipo de evaluación de riesgos de seguridad. Esos errores pueden ser tan simples como faltas de ortografía en el nombre de un entrevistado, o tan complejos como documentar incorrectamente la arquitectura del sistema actual.

5.12.4. Informe final.

El Informe final de evaluación de seguridad es la versión corregida del informe provisional. El líder del equipo debe asegurarse que este informe contenga las correcciones del proyecto que se han discutido con el cliente, por lo tanto es importante aclarar, que no es necesario que las conclusiones del informe final sean aceptadas o aprobadas por el cliente, ya que es recomendable que se discutan con él mismo y se dé la oportunidad de aclarar cualquier malentendido.

El equipo debe asegurarse de que la evaluación de seguridad final esté documentada con las conclusiones del equipo de evaluación de riesgos.

5.12.5. Plan de acción

La fase final de una evaluación de riesgos de seguridad debe propiciar que la organización cree un plan de acción encaminado a remediar todos los riesgos de seguridad identificados en el reporte final. Es conveniente asignar cada riesgo a un elemento del equipo al que se le hará responsable de implementar las medidas sugeridas en la evaluación, se debe definir una fecha para ser completado, y sus resultados deber ser monitoreados regularmente. Cada uno de estos riesgos identificados deberá ser reducido, aceptado, rechazado o asignado. Una buena práctica es grabar la medida que se aplicará al riesgo en una copia maestra del reporte de evaluación final de seguridad, con la fecha y la firma de la dirección que escogió aceptar un riesgo residual identificado, en vez de implementar la medida de corrección propuesta, si existiera tal caso.

CONCLUSIONES

Conclusiones

En México existe una carencia y deficiencia en la difusión, capacitación y fomento de la seguridad informática, desde la organización misma hasta los empleados. Esto tiene como consecuencia estar en desventaja frente a los riesgos más comunes, concentrándose especialmente en los virus y hackers, dejando en segundo término la planeación de la seguridad, las políticas y procedimientos, la capacitación y educación, la disponibilidad de los sistemas; así como, las auditorías y evaluaciones de riesgos.

Hoy en día las organizaciones son conscientes de la necesidad de identificar los riesgos asociados a TI, pero también es un hecho que al tener esta preocupación y no aplicar una metodología adecuada para cada negocio, es decir; entendiendo su cultura organizacional, sus procesos, sus operaciones críticas, es imposible lograr que estas metodologías alcancen el propósito de minimizar los riesgos.

Es por esta razón que además de conocer estándares, normas y regulaciones, es recomendable llevar a cabo una metodología de análisis y evaluación de riesgos que identifique claramente las directrices estratégicas para mitigar, aceptar, reducir o transferir dichos riesgos.

Proteger los activos más valiosos de las empresas o instituciones, frente a posibles amenazas permanentes en el medio, es un gran desafío. Este interés crece aún más cuando la información cobra importancia para sobrevivir frente a la competencia y permanecer en el mercado.

Habiendo establecido un panorama de la problemática de los riesgos en Tecnologías de Información, hemos realizado una revisión de las guías y estándares internacionales de más uso, tales como: COBIT, ISO 27001, MAAGTICSI (Nacional), etc. De éstas y otras fuentes de apoyo hemos extraído y analizado los elementos más útiles referentes a un análisis y evaluación de riesgos en Tecnologías de Información, observando que algunas de las metodologías encontradas enfatizan más en el aspecto técnico, mientras que otras más en el aspecto de la gestión y algunas otras con un equilibrio entre ambos aspectos.

Finalmente se ha desarrollado una metodología de análisis y evaluación de riesgos en Tecnologías de Información, con el propósito de cubrir con los objetivos de seguridad de las empresas o instituciones; así como en la capacitación a personas y equipos para que participen efectivamente en cualquier esfuerzo de evaluación de riesgos de seguridad.

Dicha metodología contempla seis etapas fundamentales

1. Definición del proyecto.
2. Preparación del proyecto.
3. Recolección de datos físicos, técnicos y administrativos para la evaluación.
4. Análisis de los riesgos de seguridad.
5. Mitigación de los riesgos de seguridad.
6. Recomendaciones para el reporte final.

Para definir esta metodología de análisis y evaluación de riesgos en Tecnologías de Información se tuvo en cuenta las tres dimensiones fundamentales que componen una organización informática a nivel mundial: Los procesos, las personas y la tecnología; sin olvidar que la parte más importante son las personas, mismas que hacen que los procesos y la tecnología funcionen.

El resultado de una evaluación de riesgos debe servir para hacer un inventario de acciones, con el fin de diseñar, mantener o mejorar los controles de riesgos, con esto la organización tiene en sus manos una herramienta inmejorable para el tratamiento de sus vulnerabilidades y además un diagnóstico general sobre el estado de la seguridad de su entorno: físico, lógico, de operaciones y de su infraestructura. A partir de este momento es posible establecer políticas para la corrección de los problemas ya detectados y la gestión de seguridad de ellos, para garantizar que las vulnerabilidades encontradas anteriormente no generen mayores problemas en la operación de la empresa, gestionando de esa manera la posibilidad de mitigar o eliminar nuevas debilidades que puedan surgir a lo largo del tiempo.

Cuando una evaluación de riesgos es usada como base para tomar decisiones respecto a la seguridad, la calidad de dicha evaluación se convierte en crítica. Un método de evaluación de riesgos en seguridad poco estricto puede conducir a conclusiones falsas y posteriormente a errores significativos en la planificación e incrementar los riesgos de seguridad.

La importancia de la evaluación de riesgos en la seguridad y un método de calidad para realizarla, es la razón fundamental de la presente tesis. La evaluación de riesgos en la seguridad de la información no debe ser realizada exclusivamente para completar una lista de tareas o solamente para satisfacer un requerimiento regulatorio. Una evaluación de este tipo debe ser realizada de manera profesional para entregar resultados precisos.

A continuación se listan algunos puntos clave que destacan la importancia de una evaluación de riesgos en tecnologías de información.

1. El principal objetivo de una evaluación de riesgos, como primera ley de la naturaleza, es garantizar la supervivencia de la organización, minimizando los costos asociados con los riesgos, siendo que muchos de los defectos en la administración de riesgos radica en la ausencia de objetivos claros.

2. La evaluación de riesgos en tecnologías de información es importante ya que aproxima en forma ordenada el comportamiento de los riesgos, anticipando posibles pérdidas accidentales con el diseño e implementación de procedimientos que minimicen la ocurrencia o el impacto financiero de pérdidas que pudiesen ocurrir.

3. La evaluación de riesgos en tecnologías de información, es una herramienta muy útil para el mejor desarrollo de las actividades de todos y cada uno de los departamentos de las organizaciones; en particular del departamento de sistemas de información.

4. El análisis de riesgos en Tecnologías de nformaciIón, ha contribuido a ampliar aún más los conocimientos sobre los problemas significativos que pueda tener el área de sistemas de una empresa y sobre las múltiples ideas de soluciones que se pudieran aplicar.

5. La implementación de controles de seguridad se debe justificar con base a las conclusiones obtenidas del análisis, evaluación y tratamiento de riesgos a los cuales se someten los activos de la organización.

6. Este trabajo tiene como una de sus metas primordiales el orientar a las generaciones futuras, sobre los aspectos importantes que se deben considerar en una evaluación de riesgos en Tecnologías de Información en cualquier empresa que haga uso de éstas.

7. Es importante comprender que incluso el análisis más profundo y completo no puede identificar correctamente todos los riesgos y probabilidades; se requiere control e iteraciones.

“Los riesgos son dinámicos y deben ser monitoreados permanentemente

APÉNDICE

APÉNDICE A

Mediciones de riesgo.

Una vez identificados los riesgos, el siguiente paso es decidir cómo catalogarlos. Todas las organizaciones tienen presupuestos limitados por lo que no pueden responder a cada riesgo potencial. Este análisis de riesgos permite a las organizaciones decidir cuales requieren mayor atención. Es conveniente no prestar atención y recursos para mitigar riesgos que posiblemente no ocurran y que el daño sería mínimo si ocurriesen. En cambio, debemos mitigar los riesgos que son probables de su ocurrencia y que pudieran causar un mayor daño.

Las organizaciones usan dos tipos de análisis de riesgos, estos son:

- Análisis cualitativo de riesgo.
- Análisis cuantitativo de riesgo.

Análisis cualitativo de riesgo.

Este tipo de análisis utiliza calificaciones relativas para determinar respuestas a los riesgos y maneja la probabilidad de riesgos e impacto de los mismos. La probabilidad de riesgo es importante porque mide qué tan factible es que ocurra un riesgo. Cuando se usa este tipo de evaluación se expresa la probabilidad de riesgos con medidas relativas, de la siguiente manera:

- Probabilidad alta. Muy probable de ocurrir.
- Probabilidad promedio. No muy frecuente o rara vez ocurrirá.
- Probabilidad baja. Rara vez ocurrirá.

Por supuesto que un riesgo con probabilidad alta requiere de mayor atención que uno con probabilidad baja. Otra manera de enfocar este tipo de evaluación es mediante el impacto del riesgo; esto es, el riesgo se mide por la afectación a la organización o al proyecto. El rango de calificaciones es de bajo (despreciable) a alto (sustancial); es obvio que un impacto alto requiere de mayor atención que uno bajo.

El anterior tratamiento de riesgos, puede o no ser aplicable a cualquier organización. El análisis de riesgo cualitativo prioriza los riesgos para realizar una planeación enfocada y un análisis más detallado de los mismos y así poder abordarlos

Análisis cuantitativo de riesgos

El análisis cuantitativo de riesgos es otro método de análisis; utiliza fórmulas matemáticas y números con objeto de calificar la severidad de los riesgos. El enfoque cuantitativo procura cuantificar la magnitud del riesgo, su probabilidad, identifica los riesgos de alto impacto y desarrolla planes basados en los riesgos.

Este método se enfoca principalmente en cuantificar los riesgos más altos, dado que no es práctico para aquellos de bajo impacto o poca probabilidad de ocurrencia.

El análisis cuantitativo presenta los siguientes pasos a seguir:

1. Calcular la exposición al riesgo.
   a. Asignar valor a cada recurso (activo).
   b. Determinar el porcentaje de pérdida para cada posible amenaza. Este valor es el **factor de exposición** (FE) para la amenaza, en función al recurso.

2. Calcular, para una sola vez, la pérdida para la ocurrencia de una amenaza, llamada Pérdida Única Esperada (PUE) usando la siguiente fórmula:

$$\text{PUE} = \text{Valor del recurso X FE}$$

3. Calcular o determinar la probabilidad anual de una pérdida. La probabilidad anual estimada de que dicha amenaza se materialice, es llamada la **tasa anual de ocurrencia (TAO).**

4. Calcular la pérdida anual estimada debido a una amenaza específica, llamada **pérdida esperada anual (PEA),** usando la siguiente fórmula:

$$\text{PEA} = \text{TAO X PUE}$$

La siguiente tabla contiene algunos riesgos de muestra, y el PEA calculado para cada riesgo. Ya que se tiene el PEA para cada riesgo, la organización determinará qué riesgo se abordará primero.

ANÁLISIS DE RIESGO CUANTITATIVO						
RECURSO	**RIESGO**	**VALOR**	**FE**	**PUE**	**TAO**	**PEA**
Edificio	Incendio	$700,000.00	0.60	$420,000.00	0.20	$84,000.00
Servidor de archivos	Daño físico en disco	$50,000.00	0.50	$25,000.00	0.20	$5,000.00
Datos confidenciales	Robo	$200,000.00	0.90	$180,000.00	0.70	$126,000.00
Conexión a Internet del E-business	Caída por una hora	$15,000.00	1.00	$15,000.00	12.00	$180,000.00

APÉNDICE B

Formato de control de riesgos en Tecnologías de Información

GLOSARIO

GLOSARIO

TÉRMINO	SIGNIFICADO Y/O DESCRIPCIÓN
adware	Cualquier paquete de software que automáticamente reproduce, muestra o descarga material publicitario en una computadora después de que se instala o mientras la aplicación está en uso. En la mayoría de los casos, esto ocurre sin hacer ninguna notificación al usuario o sin consentimiento del usuario. El término «adware» también se puede referir a software que muestra anuncios publicitarios, con o sin el consentimiento del usuario; como alternativa a los cargos por registro para el uso de *shareware*. Se clasifican como *adware* en el sentido de software apoyado con propaganda, pero no como «spyware». El *adware* de esta forma no opera clandes-tinamente ni engaña al usuario, y le proporciona un servicio específico.
análisis de riesgos	El procedimiento inicial de la gestión de riesgos: analizar el valor de los activos para el negocio, identificar las amenazas para esos activos y evaluar cuán vulnerable es cada activo frente a esas amenazas. La norma de seguridad de la información ISO/IEC 27001 define el análisis de riesgos como el uso sistemático de información para identificar fuentes de riesgo y realizar su estimación. [ISO/ffiC Guía 73:2002]
archivo en suspenso	Un archivo informático para guardar información (por ejemplo, transac-ciones, pagos u otros eventos) hasta que se determine la disposición apropiada de esa información. Una vez determinada la disposición apro-piada del elemento, se debería retirar del archivo en suspenso y procesar de acuerdo con los procedimientos apropiados para esa transacción parti-cular. Dos ejemplos de los elementos que se pueden incluir en un archivo en suspenso son el recibo de un pago proveniente de una fuente aún no identificada o los datos para los que aún no se haya identificado un par durante la migración hacia la nueva aplicación.
auditoría comprensiva	Una auditoría diseñada para determinar la exactitud de los registros financieros, así como también para evaluar los controles internos de una función o de un departamento.
autoridad de certificación (CA)	Es una entidad que maneja cuestiones de certificados digitales para terceros, es un certificado que da testimonio al proveer un par de llaves pública/ privada para la autenticidad de su propietario, entidad o persona a quien se le haya dado. El proceso involucra una CA que toma una decisión de emitir un certificado basado en evidencia o conocimiento obtenido para verificar la identidad del destinatario.

	Después de verificar la identidad del destinatario, la CA firma el certificado con su llave privada para su distribución al usuario, donde, después de su recibo, el usuario desencriptará el certificado con la llave pública de la CA (por ejemplo, CA comerciales, tales como Verisign proveen llaves públicas en los navegadores (browsers) de la Web). La CA ideal es autoritativa (alguien en quien confía el usuario) para el nombre o espacio clave que representa.

autoridad de registro (RA)	Una entidad opcional separada de una CA (*Certificate Authority*) que podría ser usada por una CA con una base muy grande de clientes. Las CA usan RA (*Registration Authority*) para delegar algunas de las funciones adminis-trativas asociadas con el registro o la verificación de alguna información o la totalidad de ésta que una CA necesita para emitir certificados o CRL (*Certificate Revocation List*) y para efectuar otras funciones de gestión de certificados. Sin embargo, con este arreglo la CA aún retiene la responsa-bilidad exclusiva de firmar, o bien certificados digitales o CRL. Si una RA no estuviera presente en la estructura establecida de PKI (*Public Key Infraestructure*), se asume que la CA tiene el mismo conjunto de capacidades que las definidas para una RA.

backbone	El principal canal de comunicaciones de una red digital. La parte de una red que maneja el tráfico más importante. Emplea las vías de transmisión de más alta velocidad de la red y también puede recorrer las distancias más largas. Las redes más pequeñas se adjuntan al *backbone*, y las redes que se conectan directamente al usuario final o cliente se denominan «redes de acceso». Un backbone puede abarcar un área geográfica de cualquier tamaño, desde un edificio hasta un complejo de oficinas o hasta un país entero, o puede ser tan pequeño como un *backplane* en un gabinete.

base de datos jerárquica	Es una base de datos estructurada en una relación árbol/raíz o padre/hijo. Cada padre puede tener muchos hijos, pero cada hijo puede tener sólo un padre.

BIA	(*Business Impact Analysis*) Análisis de impacto del negocio. Es el proceso para determinar el impacto de perder el respaldo de cualquier recurso. El estudio de evaluación del análisis del impacto en el negocio establecerá el incremento de esa pérdida en el tiempo. Se basa en el hecho de que la gerencia principal, cuando se le brindan datos fiables para documentar el impacto potencial de un recurso perdido, puede tomar la decisión apropiada.

calidad del software	Grado en el que un cliente o usuario percibe que el software satisface sus expectativas.

call center	Centro de atención de llamadas entrantes (*Inbound*) o salientes (*outbound*) es una herramienta de comunicación y relación con los clientes que utiliza el teléfono como medio de comunicación básico gestionado por «personas humanas» en conjunto con los recursos humanos, físicos y tecnológicos necesarios y disponibles, basados en metodologías de trabajo y procesos determinados y adecuados, para atender las necesidades y dar servicio a cada «cliente único» con el objeto de atraerlos y fidelizarlos con la organización y permitir su viabilidad.

cambios de alcance (*scope creep*)	También denominado cambio gradual de requerimientos, se refiere a los cambios no controlados del alcance en un proyecto. Este fenómeno puede ocurrir cuando no se define, documenta y controla de manera apropiada el alcance de un proyecto. Por lo general, la expansión del alcance consta de productos nuevos o funciones nuevas de productos ya aprobados. Por lo tanto, el equipo del proyecto se desvía de su propósito inicial. Debido a la tendencia generalizada a centrarse en una sola dimensión de un proyecto, el cambio de alcance también puede hacer que el equipo del proyecto exceda el presupuesto y programa originales. Por ejemplo, el cambio de alcance puede ser el resultado de un control de cambios deficiente, de una falta de identificación apropiada de los productos y funciones que se necesitan para lograr los objetivos del proyecto en primera instancia, o de un gerente de proyectos o patrocinador ejecutivo débil.

caso base (*base case*)	Un cuerpo de datos estandarizados creado con fines de prueba. Los usua-rios por lo general establecen los datos. Caso base valida los sistemas de aplicación en producción y prueba la operación exacta del sistema que se está llevando a cabo.

caso de negocio (*business case*)	Un documento que provee gestión con suficiente información, necesaria para permitir decidir si se soporta un proyecto propuesto, antes de que se cause inestabilidad de recursos significativos para su desarrollo. Un caso de negocio (*business case*) incluye el análisis de desempeño corriente del proceso de negocio; supuestos, necesidades o problemas asociados; soluciones pro-puestas y limitaciones potenciales, basadas en un análisis de rentabilidad ajustado al riesgo.

CCTA	Agencia central de Informática y telecomunicaciones del Gobierno Británico: *Central Computer and Telecommunications Agency*.

CCTV	Circuito Cerrado de Televisión, acrónimo en inglés de *Closed Circuit Television* Es una tecnología de video vigilancia visual, diseñada para supervisar una diversidad de ambientes y actividades.

CEO	Director Ejecutivo o Director General; acrónimo en inglés: Chief Executive Officer. Es el de más alto rango o administrador a cargo del total de la gestión de una organización .

CGI	(*Common Gateway Interface*) Es la utilización de un pequeño programa que permite comunicarse con un servidor Web.

CISA	Auditor certificado en sistemas de información, acrónimo en inglés de *Certified Information Systems Auditor*. Es una certificación para auditores en sistemas de información, respaldada por ISACA (**Information Systems Audit and Control Association**).

CLM	(*Council of Logistics Management*) El Concilio de Administración Logística define a la logística como «la parte del proceso de la cadena de abastecimiento que planea, implementa y controla eficiente y efectivamente el flujo y almacenamiento de bienes, servicios e información relacionada, desde el punto de origen hasta el de consumo, para así satisfacer las necesidades del cliente». Cuando se considera de forma amplia el campo de la logística, se tiene que incluir el transporte de personas.

CMM	(*Capability Maturity Module*) Modelo de evaluación de los procesos de una organización. Fue desarrollado inicialmente para los procesos relativos al desarrollo e implementación de software por la Universidad Carnegie-Mellon para el SEI.

COBIT	Objetivos de Control para Tecnología de la Información y Relacionada, acrónimo en inglés de *Control Objectives for Information and Related Technology*. Es una guía de mejores prácticas presentada como infraestructura digital, dirigida a la gestión de tecnología de la información.

cold-site	Un sitio de respaldo de SI que tiene los componentes eléctricos y físicos necesarios de un centro de cómputo, pero que no tiene instalado el equipo de cómputo. El lugar está listo para recibir el equipo de reemplazo necesario en el caso de que los usuarios tengan que trasladarse desde su lugar principal de procesamiento al sitio alterno.

completitud	Debe contener todos aquellos hechos que pudieran ser importantes.

concisión	Brevedad y economía de medios en el modo de expresar un concepto con exactitud.

concreción	Reducción a lo esencial o a lo preciso de un asunto o materia.

conectividad	Capacidad de un dispositivo (una PC, periférico, PDA, móvil, robot, electro-doméstico, coche, etc.) de poder ser conectado (generalmente a una PC u otro dispositivo) sin la necesidad de una computadora, es decir, en forma autónoma.

conmutación de mensajes	Es una metodología para controlar el tráfico de las telecomunicaciones, en la que un mensaje completo es enviado a un punto de concentración y almacenado allí hasta que se establezca la vía de comunicación.

conmutación de paquetes	Es el proceso de transmitir mensajes en partes convenientes que puedan ser armadas nuevamente al llegar a su destino.

consistencia	Ausencia de contradicciones.

Contramedida	Representa la acción para prevenir una amenaza. Las contramedidas que deben implementarse no solamente son soluciones técnicas, sino también reflejan la capacitación y la toma de conciencia por parte del usuario, además son reglas claramente definidas.

Contraseña	Una cadena de caracteres generalmente cifrados (encriptados) y protegidos que autentican a un usuario ante el sistema de cómputo.

contrato de no revelación (NDA)	También denominado contrato de confidencialidad (CDA), o contrato de no divulgación, es un contrato legal entre por lo menos dos partes que describe materiales confidenciales que las partes desean compartir entre sí para cier-tos propósitos, pero que desean restringir del uso generalizado. En otras palabras, es un contrato a través del cual las partes acuerdan no divulgar información cubierta por el contrato. Un NDA crea una relación confidencial entre las partes para proteger cualquier tipo de secreto comercial. Como tal, un NDA puede proteger información no pública de negocios. En el caso de ciertas entidades gubernamentales, la confidencialidad de información no relacionada con secretos comerciales puede estar

	sujeta a requerimientos regulatorios aplicables y, en algunos casos, se puede requerir que se revele a una parte externa que solicite la información. Generalmente, la entidad gubernamental incluirá una disposición en el contrato que permita al vendedor revisar una solicitud de información que el vendedor identifica como confidencial y el vendedor puede apelar esa decisión y solicitar la divulgación.

controlador frontera de sesiones (SBC)	Proporciona funciones de seguridad para el tráfico en redes VoIP (VoIP es el conjunto de normas, dispositivos, protocolos, en definitiva la *tecnología* que permite comunicar voz sobre el protocolo IP) similares a las de los firewalls. Los SBC se pueden configurar para funcionar como filtros de protocolos VoIP específicos, monitorear ataques de negación de servicio (DoS, Denial of service) y proporcionar funciones de dirección de red y de traducción de protocolos.

controles de edición	Detecta los errores en la porción de información que se está ingresando a la computadora para su procesamiento. Los controles pueden ser manuales o automatizados y permiten al usuario editar los errores de datos antes de que éstos sean procesados.

core business	Corazón del negocio. Es el conjunto de actividades que realiza una empresa y que la caracterizan definen y diferencian en el mercado.

core processes	Procesos clave que son fundamentales en una empresa para garantizar la continuación de la competitividad.

COSO	(*Committee Of Sponsoring Organizations*) nuevo concepto de control interno donde se brinda una estructura común, el cual es documentado en el deno-minado informe COSO.

CRAMM	Método de Gestión y Análisis de Riesgos de la Agencia Central de Informática y Telecomunicaciones del Gobierno Británico, acrónimo de *CCTA Risk Analysis and Management Method*; fue desarrollado por el gobierno británico en 1985.

Criptografía	Se encarga del estudio de los algoritmos, protocolos y sistemas que se utilizan para dotar de seguridad a las comunicaciones, a la información y a las entidades que se comunican.

criptosistema (cifrosistema) de llave pública	Usado en el cifrado (en la encriptación) de datos, usa una llave de encrip-tación (cifrado), como una llave pública, para encriptar (cifrar) el texto normal en texto encriptado (cifrado). Usa la llave diferente de desencriptación (descifrado), como una llave secreta, para desencriptar (descifrar) el texto encriptado (cifrado) en el texto normal correspondiente. En contraste con un criptosistema (cifrosistema) de llave privada, la llave de desencriptación (descifrado) debe ser secreta; sin embargo, la llave de encriptación (cifrado) puede ser conocida por todos. En un criptosistema (cifrosistema) de llave pública, dos llaves son asimétricas de modo que la llave de encriptación (cifrado) no sea equivalente a la llave de descifrado (desencriptación).

CRM	(*Customer Relationship Management*), Administración de la relación con el cliente. Estrategia de negocio orientada a la satisfacción del cliente. Se le pueden asociar varios significados: 1. La administración basada en la relación con los clientes. CRM es un modelo de gestión de toda la organización, basada en la orientación al cliente (u orientación al mercado según otros autores), el concepto más cercano es *Marketing relacional* (según se usa en España) y tiene mucha relación con otros conceptos como: *Clienting, Marketing* 1x1, *Marketing* directo de base de datos, etcétera. 2. La administración de la relación con los clientes. CRM es sinónimo de Servicio al cliente, o de Gestión de clientes. Con este significado CRM se refiere sólo a una parte de la gestión de la empresa. 3. Software para la administración de la relación con los clientes. Sistemas informáticos de apoyo a la gestión de las relaciones con los clientes, a la venta y al marketing. Con este significado CRM se refiere al sistema que administra un *Data warehouse* (Almacén de Datos) con la información de la gestión de ventas y de los clientes de la empresa.

CSCMP	*Council of Supply Chain Management Professionals* define a la *Supply Chain* (Cadena de Suministro o Cadena de Abastecimiento) como: 1. La Cadena de Suministro une a muchas compañías, iniciando con mate-rias primas no procesadas y terminando con el consumidor final utilizando los productos terminados; y 2. Todos los proveedores de bienes y servicios y todos los clientes están unidos por la demanda de los consumidores de productos terminados, al igual que los intercambios materiales e informáticos en el proceso *logístico*, desde la adquisición de materias primas hasta la entrega de productos terminados al usuario final.

CTI	Centro de Tecnología de Información.

Checksums/ suma de verificación o suma de chequeo	Es una función hash que tienen como propósito principal detectar cambios accidentales en una secuencia de datos para proteger la integridad de éstos, verificando que no haya discrepancias entre los valores obtenidos al hacer una comprobación inicial y otra final tras la transmisión.

***Data Warehouse*, (DW)**	(Almacén de datos). Es un conjunto de datos integrados, no transaccionales, no volátiles, orientados a un tema específico, variables en el tiempo y que se utilizan para el apoyo al proceso de toma de decisiones.

Data Warehousing (DW)	Almacén de datos o proceso mediante el cual las empresas extraen sentido y significado a sus datos a través del uso de un DW.

derechos de acceso	También llamados permisos o privilegios. Estos son los derechos otorgados a los usuarios por el gerente o por el supervisor. Los derechos de acceso determinan las acciones que pueden ejecutar los usuarios, por ejemplo, leer, grabar, ejecutar, crear, eliminar en los archivos en los volúmenes compartidos o partes de los archivos en el servidor.

directrices	Guías de acción. Instrucciones o normas generales para la ejecución de algo.

diseño *(layout)* del archivo	Especifica la longitud del registro del archivo y la secuencia y el tamaño de sus campos. El diseño del archivo especificará también el tipo de datos con-tenidos dentro de cada campo. Por ejemplo, datos alfanuméricos, decimales por zona, empaquetados y binarios son tipos de datos.

DRP	Plan de recuperación de desastres, acrónimo en inglés de *Disaster Recovery Plan*. Es la estrategia que se seguirá para restablecer los servicios de TI (Hardware y Software) después de haber sufrido un daño por una catástrofe natural, terremoto, falla masiva, daño premeditado, ataque de cualquier tipo, el cual atente contra la continuidad del negocio.

DSS	*(Decision Support Systems)* Sistemas para el Soporte de Decisiones. A través de estos sistemas, el usuario puede responder de manera más concreta en la toma de decisiones, ya que le brindan una panorámica sobre el problema y una serie de alternativas propias para su resolución.

e-commerce	*(electronic commerce)* Comercio electrónico

EEPROM o E²PROM	Acrónimo en inglés de "*Erasable Programmable Read Only Memory*" que se puede traducir como Memoria programable borrable de sólo lectura. Es un tipo de memoria ROM que puede ser programada, borrada y reprogramada eléctricamente. Son memorias no volátiles.

eficiencia	Es la óptima utilización de los recursos disponibles para la obtención de resultados deseados.

EIS	*(Executive Information Systems).* Sistemas de Información para Ejecutivos son sistemas computarizados que proveen a los ejecutivos un fácil acceso a información interna y externa que es relevante para sus factores críticos de éxito. Este concepto nació de la demanda de sistemas de información que respondieran a las necesidades reales de los ejecutivos en las organizacio-nes apoyándolos en la resolución de problemas no estructurados basándose en fuentes de información internas y externas, con la facilidad de resumir, filtrar, comprimir y rastrear datos críticos para las organizaciones.

ergonómico	Cuando está hecho para la comodidad o seguridad del usuario.

ERP	*(Enterprise Resource Planning)* Planificación de Recursos Empresariales. Son sistemas de información gerenciales que integran y manejan muchos de los negocios asociados con las operaciones de producción y de los aspectos de distribución de una compañía comprometida en la producción de bienes o servicios.

escalabilidad	Propiedad deseable de un sistema, una red o un proceso, que indica su habilidad, o bien, para manejar el crecimiento continuo de trabajo de manera fluida, o bien, para estar preparado para hacerse más grande sin perder calidad en los servicios ofrecidos.

estructura de datos	Son las relaciones entre los archivos en una base de datos y entre los elementos de datos dentro de cada archivo.

ETL	*(Extract Transform and Load)* Extraer Transformar y Cargar.

exactitud	Capacidad de un instrumento de medir un valor cercano al valor de la magnitud real.

extensibilidad	Facultad de adaptar software a los cambios que se especifiquen.

FAA	Administración Federal de Aviación, acrónimo en inglés de *Federal Aviation Administration*. Es la entidad gubernamental responsable de la regulación de todos los aspectos de la aviación civil en los Estados Unidos.

FATI	Función de Auditoría a Tecnologías de Información (FATI)

FDDI	(*Fiber Distributed Data Interface*) Las redes Interfaz de Datos Distribuida por Fibra surgieron a mediados de los años ochenta para dar soporte a las estaciones de trabajo de alta velocidad, que habían llevado las capacidades de las tecnologías Ethernet y Token Ring existentes hasta el límite de sus posibilidades.

FEC	Factores Críticos de Éxito.

fiabilidad	Probabilidad de que el dispositivo desarrolle una determinada función bajo ciertas condiciones y durante un período de tiempo determinado.

Firewall	Su traducción al español es: Cortafuego. Puede ser implementado en hardware o software, o una combinación de ambos. Los cortafuegos se utilizan con frecuencia para evitar que los usuarios de Internet no autorizados tengan acceso a redes privadas conectadas a Internet, especialmente intranets.

Firmware	Es un bloque de instrucciones de máquina para propósitos específicos, grabado en una memoria, normalmente de lectura/escritura (ROM, EEPROM, flash, etc.), que establece la lógica de más bajo nivel que controla los circuitos electrónicos de un dispositivo de cualquier tipo.

flexibilidad	Capacidad de adaptarse rápidamente a las circunstancias.

FRAP	Acrónimo en ingles de *Facilitated Risk Assessment Process. Es el* Proceso de Evaluación de Riesgos Facilitado. Fue desarrollado por Tom Peltier en 2001 y diseñado como una metodología que podría ser utilizada por los propios directivos, con la guía de un profesional capacitado.

FTP	*(Foiled Twisted Pair)* Par torcido blindado general. Tipo de alambre. El FTP cuenta con un blindaje de aluminio que envuelve a los pares para dar una mayor protección contra las emisiones electromagnéticas del exterior.

GPS	*(Global Positioning System)* Sistema de Posicionamiento Global

GS	*(Groupware Systems)* Programa Informático Colaborativo, integra el trabajo en un solo proyecto con muchos usuarios concurrentes que se encuentran en diversas estaciones de trabajo, conectadas a través de una red (Internet o Intranet), dentro de la cual se envían mensajes, archivos, datos o documentos y facilitan compartir información.

GUI	*(Graphic User Interface)* Interfaz gráfica de usuario. Es el conjunto de méto-dos y formas que permiten la interacción de un sistema con el usuario, utilizando gráficos e imágenes.

Hacker	En el mundo de la informática, un hacker es una persona que entra de forma no autorizada a computadoras y redes de computadoras. Su motivación varía de acuerdo a su ideología: fines de lucro, como una forma de protesta o simplemente por la satisfacción de lograrlo. Los hackers han evolucionado de ser grupos clandestinos a ser comunidades con identidad bien definida. De acuerdo a los objetivos que un hacker tiene, y para identificar las ideas con las que comulgan, se clasifican principalmente en: hackers de sombrero negro, de sombrero gris, de sombrero blanco y *script kiddie*.

Hackers de sombrero negro	Se le llama hacker de sombrero negro a aquel que penetra la seguridad de sistemas para obtener una ganancia personal o simplemente por malicia. La clasificación proviene de la identificación de villanos en las películas antiguas del vejo oeste, que usaban típicamente sombreros negros.

Hackers de sombrero blanco	Se le llama hacker de sombrero blanco a aquel que penetra la seguridad de sistemas para encontrar puntos vulnerables. La clasificación proviene de la identificación de héroes en las películas antiguas del viejo oeste, que usaban típicamente sombreros blancos.

Hackers de sombrero gris	Como el nombre sugiere, se le llama hacker de sombrero gris a aquel que es una combinación de sombrero blanco con sombrero negro, dicho en otras palabras: que tiene ética ambigua. Pudiera tratarse de individuos que buscan vulnerabilidades en sistemas y redes, con el fin de luego ofrecer sus servicios para repararlas bajo contrato.

Hacker **Script kiddies**	Se les denomina *script kiddies* a los hackers que usan programas escritos por otros para lograr acceder a redes de computadoras, y que tienen muy poco conocimiento sobre lo que está pasando internamente.

Hardware	Corresponde a todas las partes físicas y tangibles de una computadora.

Help desk	Mesa de ayuda donde se ofrecen servicios acerca de soporte técnico (bugs, consultas, reparaciones, etc.)

heurístico	(Del griego *heurisko*, hallar) Ayuda en el aprendizaje, para descubrir o resol-ver problemas utilizando la experimentación y los métodos de ensayo y error.

Holístico	Holístico implica todo aquello vinculado o perteneciente al Holismo. En tanto que el Holismo propone la siguiente idea: todas las propiedades de un sistema, aquellas que lo conforman, ya sea este biológico, químico, social, económico, entre otros, no podrán ser determinadas o explicadas por las partes que lo componen por si solas, o sea, el sistema como un todo es el que determina cómo se comportan las partes intervinientes.

HTML	*(HyperText Markup Language)* Lenguaje de Marcado de Hipertexto, es el lenguaje de marcado predominante para la elaboración de páginas Web.

HTTP	*(HyperText Transfer Protocol)* Protocolo de Transferencia de Hipertexto. Protocolo de comunicación para peticiones de acceso a páginas Web y respuesta de la misma.

HTTPS	Versión segura del protocolo http.

HVCA	Acrónimo en ingles de *Heating, Ventilating and Air Conditioning*. Sistemas de aire acondicionado, ventilación y temperatura.

IAM	Metodología de evaluación de InfoSec, acrónimo en inglés de *InfoSec Assessment Methodology*.

IDS	Sistema de Detección de Intrusos, acrónimo en inglés de *Intrusion Detection System*. Es un programa usado para detectar accesos no autorizados a un computador o a una red.

IEC	Siglas en ingles de *International Electrotechnical Commission*. Comisión Electrotécnica Internacional es una organización de normalización en los campos eléctrico, electrónico y tecnologías relacionadas. Fue fundada en 1906, siguiendo una resolución aprobada en 1904 en el Congreso Internacional Eléctrico en San Luis Missouri.

IEEE	*(The Institute of Electrical and Electronics Engineers)* Instituto de Ingenieros Eléctricos y Electrónicos, es una asociación técnico-profesional mundial dedicada a la estandarización.

ignición	Ocurre cuando el calor que emite una reacción llega a ser suficiente como para sostener la reacción química.

Informe COSO	El Informe COSO es un documento que contiene las principales directivas para la implantación, gestión y control de un sistema de Control Interno.

Ingeniería Social	Hace referencia al arte de manipular personas para eludir los sistemas de seguridad. Esta técnica consiste en obtener información de los usuarios vía telefónica, correo electrónico, correo tradicional o contacto directo.

integridad	Se refiere a las medidas de salvaguarda que se incluyen en un sistema de información para evitar la pérdida accidental de los datos.

interoperabilidad	Habilidad que tiene un sistema o producto para trabajar con otros sistemas o productos sin un esfuerzo especial por parte del cliente.

IP	Protocolo de internet, siglas de *Internet Protocol*. Es utilizado para la comunicación de datos a través de una red de paquetes combinados.

ISACA	Asociación de Auditoría y Control de Sistemas de Información, por sus siglas en ingles de *Information Systems Audit and Control Association*. Apoya y patrocina el desarrollo de metodologías y certificaciones para la realización de actividades de auditoría y control en sistemas de información.

ISO	Organización Internacional de Normalización, acrónimo en inglés de *International Organization for Standardization*. Es el organismo encargado de promover el desarrollo de normas internacionales de fabricación, comercio y comunicación para todas las ramas industriales a excepción de la eléctrica y la electrónica.

ITGI	Siglas en ingles de *IT Governance Institute*. El Instituto de Gobierno de TI de ISACA, que se estableció en 1998, en reconocimiento a la creciente importancia de la tecnología de información para el éxito de las empresas.

ITIL	(*Information Technology Infrastructure Library*) Biblioteca de Infraestructura de Tecnologías de Información; los términos y su uso se extienden con la popularización del estándar ITIL, para el gerenciamiento de TI.

KBS	*(Knowledge Based Systems)* Sistemas Basados en el Conocimiento, son sistemas avanzados de representación y resolución de problemas com-plejos. Su arquitectura y sus formalismos de representación son la base de muchos de los sistemas actuales. Su uso se puede encontrar en todas las ramas de aplicaciones especiales de los sistemas informáticos donde se requieran prestaciones especiales, sobre todo en aquellas áreas donde el conocimiento de expertos sea el soporte básico como medicina, industria, gestión, finanzas, organización empresarial y otros.

KPI	*(Key Performance Indicators)* Indicadores clave de desempeño. Miden el nivel de desempeño de un proceso, e indican qué tan buenos son los procesos, de manera que se pueda alcanzar el objetivo propuesto.

LSSI	Ley de Servicios de la Sociedad de la Información que desde 2002 vino a poner un poco de orden en Internet (con unos años de retraso tras la explosión de la burbuja de Internet en 1999-2000), establece las bases para garantizar nuestros derechos como consumidores en las compras y servicios *online*.

MAAGTICSI	Manual Administrativo de Aplicación General en Materia de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información.

mainframe	Computadora central (macrocomputadora). Computadora grande poderosa y costosa utilizada principalmente en empresas que

	necesitan procesar gran cantidad de datos o soportar gran cantidad de usuarios.

Mark Zuckerberg (Filántropo de USA)	Director operativo de Facebook, nace el 17/Feb/85. Ridículamente joven para ser multimillonario, recuerda que fundó Facebook cuando era adolescente. Inspiró a una de cada siete personas en el planeta a usar su producto y cambió la forma en la que el mundo se comunica, todo antes de los 30 años.

MDDC	Minería de Datos para el Descubrimiento de Conocimiento.

MDP	Minería de Datos Predictiva.

Metadata	Datos que describen otros datos.

Microelectrónica	Tecnología mediante la cual se diseñan dispositivos electrónicos empacados en grandes densidades en una pastilla única de semiconductor.

migración	Proceso consistente en hacer que los datos y las aplicaciones existentes funcionen en una computadora, software o sistema operativo distinto.

minería de datos	Mecanismo de explotación consistente en la búsqueda de información valiosa en grandes volúmenes de datos; es decir, es el análisis de archivos y bitácoras de transacciones, trabaja a nivel del conocimiento con el fin de descubrir patrones, relaciones, reglas, asociaciones o incluso excepciones útiles para la toma de decisiones.

módem	Dispositivo que sirve para enviar una señal llamada moduladora mediante otra señal llamada portadora. Se han usado módems desde los años 60, principalmente debido a que la transmisión directa de las señales electrónicas inteligibles, a largas distancias, no es eficiente, por ejemplo, para transmitir señales de audio por el aire, se requerirían antenas de gran tamaño (del orden de cientos de metros) para su correcta recepción. Es habitual encontrar en muchos módems de red conmutada la facilidad de respuesta y marcación automática, que les permiten conectarse cuando reciben una llamada de la RTPC (Red Telefónica Pública Conmutada) y proceder a la marcación de cualquier número previamente grabado por el usuario. Gracias a estas funciones se pueden realizar

	automáticamente todas las operaciones de establecimiento de la comunicación.

NIC	*(Network Interface Card)* Tarjeta de Red.

NSA	Siglas en inglés de *National Security Agency's*. Agencia de Seguridad Nacional. Es una agencia de inteligencia del Gobierno de los Estados Unidos que se encarga de todo lo relacionado con la seguridad de la información.

OCTAVE	Por sus siglas en ingles de *Operationally Critical Threat, Asset, and Vulnerability Evaluation*. El método de evaluación de vulnerabilidades, activos y amenazas críticas operacionales. Fue desarrollado por el Instituto de Ingeniería de Software de la Universidad de Carnegie Mellon.

OLAP	*(On-Line Analytical Processing)* Procesamiento analítico en línea. Es una solución utilizada en el campo de la llamada Inteligencia Empresarial (o *Business Intelligence*), cuyo objetivo es agilizar la consulta de grandes cantidades de datos.

ONG	Organizaciones no gubernamentales

OSI	*(Open System Interconnection)* El modelo de referencia de Interconexión de Sistemas Abiertos es el modelo de red descriptivo creado por la Organi-zación Internacional para la Estandarización lanzado en 1984. Es decir, es un marco de referencia para la definición de arquitecturas de interconexión de sistemas de comunicaciones.

outsoucer	Proveedor externo. Aquel que provee de servicios externos.

outsourcing	Contratación externa o «tercerización»

out-tasking	Modalidad de outsourcing enfocado hacia tareas específicas.

Parametrización	Establecer un conjunto de valores normalizados para trabajar con la informa-ción y registros con los que se alimenta un sistema.

PCS	Plan de aseguramiento de Calidad de Software

Phishing	Es el robo de información personal y financiera del usuario, a través de la falsificación de un ente de confianza. De esta forma, el usuario cree ingresar los datos en un sitio de confianza cuando, en realidad, estos son enviados directamente al atacante.

plataformas de servidor	*(*Server Platforms*)* Un término usado a menudo como sinónimo de sistema operativo, la plataforma es el hardware o software subyacentes para un sistema, es decir, el motor que dirige el servidor.

Plugins	Módulo de software o hardware que adiciona una característica o un servicio a un sistema más grande.

Portabilidad	Característica que posee un software para ejecutarse en diferentes platafor-mas, el código fuente del software es capaz de reutilizarse en vez de crearse un nuevo código cuando el software pasa de una plataforma a otra. A mayor portabilidad menor es la dependencia del software con respecto a la plataforma.

PRIMA	Acrónimo de *Prevención de Riesgos Informáticos con Metodología Abierta*. Es un conjunto de metodologías españolas desarrolladas a partir de 1990 y hasta la actualidad, con un enfoque subjetivo.

procesos en línea	Varios procesos, ejecutándose uno tras de otro.

procesos por lote	*(Modo batch)* Ejecución de un programa sin el control o supervisión directa del usuario.

PyME	Pequeñas y Medianas Empresas

RAID	Acrónimo en inglés de *Redundant Array of Independent Disks*. Es un arreglo redundante de discos independientes. Tecnología utilizada para la redundancia y la mejora del rendimiento; misma que combina varios discos físicos y los integra en una matriz lógica.

reingeniería	Revisión fundamental y el rediseño radical de los procesos de negocios para lograr mejoras dramáticas en medidas de desempeño tales como en costos, calidad, servicio y rapidez.

repositorio	(Depósito) Es un sitio donde se almacena y mantiene información digital, generalmente bases de datos o archivos informáticos.

reusabilidad	La noción de objeto permite que programas que traten las mismas estruc-turas de información reutilicen las definiciones de objetos empleadas en otros programas e incluso los procedimientos que los manipulan. De esta forma, el desarrollo de un programa puede llegar a ser una simple combinación de objetos ya definidos donde éstos están relacionados de una manera particular.

reutilización	Acción de volver a utilizar los bienes o productos.

Reversibilidad	Este concepto se refiere a la posibilidad de recuperación de los activos y servicios cedidos a la empresa de outsourcing. Tiene aplicación tanto en la terminación del periodo de vigencia del contrato como en las salidas programadas que se establezcan.

RIIOT	Revisión, Entrevistas, Inspección, Observación y Prueba; acrónimo de *Review, Interview, Inspect, Observe and Test*. Es una técnica usada en la evaluación de riesgos, para la fase de recolección de datos.

ROM	Acrónimo en inglés de "R*ead-Only Memory"*. La memoria de sólo lectura es un medio de almacenamiento utilizado en computadoras y dispositivos electrónicos, que permite sólo la lectura de la información y no su escritura, independientemente de la presencia o no de una fuente de energía.

SCSI	*(Small Computers System Interface)* Sistema de Interfaz para Pequeñas Computadoras, es una interfaz estándar para la transferencia de datos entre distintos dispositivos del bus de la computadora. Algunos profesionales lo castellanizan como escasi o escosi, por la pronunciación en inglés de su sigla, otros por el contrario prefieren deletrearlo.

SEI	*(Software Engineering Institute)* Instituto Federal Estadounidense de Inves-tigación y Desarrollo, fundado por el Congreso de los Estados Unidos en 1984 para desarrollar modelos de evaluación y mejora en el desarrollo de software, que dieran respuesta a los problemas que generaba al ejército estadounidense a la programación e integración de los subsistemas de software en la construcción de complejos sistemas militares.

sello temporal	*(Timestamp)* Registro de fecha.

service bureau	Firmas especializadas que prestan servicios de procesamiento de datos a empresas externas.

servidores de aplicaciones	*(*Application Servers*)* Designados a veces como un tipo de middleware (software que conecta dos aplicaciones), los servidores de aplicaciones ocupan una gran parte del territorio entre los servidores de bases de datos y el usuario, y a menudo los conectan.
servidores de audio/video	*(*Audio/Video Servers*)* Añaden capacidades multimedia a los sitios Web permitiéndoles mostrar contenido multimedia en forma de flujo continuo (streaming) desde el servidor.
servidores de correo	*(*Mail Servers*)* Casi tan ubicuos y cruciales como los servidores Web, los servidores de correo mueven y almacenan el correo electrónico a través de las redes corporativas (vía LAN y WAN) y de Internet.
servidores de chat	*(*Chat Servers*)* Permiten intercambiar información a una gran cantidad de usuarios ofreciendo la posibilidad de llevar a cabo diálogos en tiempo real.
servidores de fax	*(*Fax Servers*)* Un servidor de fax es una solución ideal para organizaciones que tratan de reducir el uso del teléfono pero necesitan enviar documentos vía fax.
servidores de listas	*(*List Servers*)* Ofrecen una manera mejor de administrar listas de correo electrónico, bien sean diálogos interactivos abiertos al público o listas unidireccionales de anuncios, boletines de noticias o publicidad.
servidores de noticias	*(*News Servers*)* Actúan como fuente de distribución y entrega para los millares de grupos de noticias públicas, actualmente accesibles a través de la red de noticias USENET.
servidores FTP	*(*FTP Servers*)* Uno de los servicios más antiguos de Internet, *File Transfer Protocol* permite mover uno o más archivos.
servidores *groupware*	*(*Groupware Servers*)* Un servidor Groupware es un software diseñado para permitir colaborar a los usuarios, sin importar la localización, vía Internet o vía Intranet corporativo y trabajar juntos en una atmósfera virtual.
servidores IRC	*(*IRC Servers*)* Otra opción para usuarios que buscan dialogar en tiempo real, *Internet Relay Chat* consiste en varias redes de servidores separadas que permiten que los usuarios conecten el uno al otro vía una red IRC.

servidores Proxy	*(*Proxy Servers*)* Se sitúan entre un programa del cliente (típicamente un navegador) y un servidor externo (típicamente otro servidor Web) para filtrar peticiones, mejorar el funcionamiento y compartir conexiones.

servidores Telnet	*(*Telnet Servers*)* Un servidor Telnet permite a los usuarios entrar en una computadora huésped y realizar tareas como si estuviera trabajando directamente en esa computadora.

servidores Web	*(*Web Servers*)* Básicamente, un servidor Web almacena el contenido estático a un navegador, carga un archivo y lo sirve a través de la red al navegador de un usuario. Este intercambio es mediado por el navegador y el servidor que hablan el uno con el otro mediante HTTP. Se pueden utilizar varias tecnologías en el servidor para aumentar su potencia más allá de su capacidad de entregar páginas HTML; éstas incluyen scripts CGI, seguridad SSL y páginas activas del servidor (ASP).

SFI	Acrónimo de *Sistema de Fuerza Ininterrumpible*, es un equipo cuya función principal es evitar una interrupción de voltaje en la carga a proteger. También se utiliza Uninterruptible Power Supply (UPS)*.*

SGBD	*(Data Base Management System).* Un Sistema Gestor de Bases de Datos o DBMA *(DataBase Management System)* es una colección de programas cuyo objetivo es servir de interfaz entre la base de datos, el usuario y las aplicaciones. Se compone de un lenguaje de definición de datos, de un lenguaje de manipulación de datos y de un lenguaje de consulta. Un SGBD permite definir los datos a distintos niveles de abstracción y manipular dichos datos, garantizando su seguridad e integridad.

SGML	*(Standard Generalized Markup Language)* Lenguaje de Marcado de Anota-ciones Generales. Es un metalenguaje de donde deriva el HTML y el XML. SGML desciende del GML *(Generalized Markup Language)* definido por IBM en los años 60. SGML provee una variedad de marcas que pueden ser usadas para muchas aplicaciones. Originalmente fue diseñado para el intercambio de documentos legibles por las máquinas en grandes proyectos gubernamentales, legales y de la industria aeroespacial. También ha sido usado extensamente en la industria de la impresión y la industria editorial. Pero su complejidad ha impedido que se extienda a aplicaciones de menor escala para propósito general.

SGSI	Acrónimo de Sistema de Gestión de la Seguridad de la Información.

SI	Sistema(s) de Información.

SIE	*(Executive Information Systems)* Sistemas de Información Empresarial especialistas en el desarrollo de software de administración y gestión para empresas. Facilitan al usuario la recuperación y análisis de la medida de *performance* (Desempeño con respecto al rendimiento) de la organización.

SLA	*(Service Level Agreement)* Acuerdo de Nivel de Servicio. Es un contrato escrito entre un proveedor de servicio y su cliente con objeto de fijar el nivel acordado para la calidad del servicio.

SNMP	(Simple Network Management Protocol) Protocolo Simple de Administración de Red o SNMP es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. Es parte de la familia de protocolos TCP/IP. SNMP permite a los administra-dores supervisar el funcionamiento de la red, buscar y resolver sus problemas, y planear su crecimiento.

software	Se refiere al equipamiento lógico o soporte lógico de una computadora digital, y comprende el conjunto de los componentes lógicos necesarios para hacer posible la realización de una tarea específica.

SQA	*(Software Quality Assurance)* Aseguramiento de la calidad del software consiste en un medio de control de la ingeniería de software (ACS), procesos y métodos utilizados para asegurar la calidad. Los métodos por los cuales esto se lleva a cabo son muchos y variados, y puede incluir la garantía de la conformidad con una o varias normas, tales como ISO 9000 o un modelo como CMMI. El SQA aportará la confianza en que el producto (software) satisfará los requisitos dados de calidad y la adhesión a las normas de productos de software, procesos y procedimentos. El ACS incluye el proceso de asegurar el establecimiento de estándares y procedimientos y que éstos se sigan durante todo el ciclo de adquisición de software.

SRM	Acrónimo en inglés de *Security Risk Management*, Gestión de riesgos de seguridad.

SSH	*(Secure Shell)* Protocolo para facilitar la comunicación segura entre dos sistemas usando una arquitectura cliente/servidor y permite a los usuarios conectarse a un host remotamente.

SSID	*(Service Set Identifier)* Identificación de set de servicios, es un nombre incluido en todos los paquetes de una red inalámbrica (Wi-Fi) para identi-ficarlos como parte de esa red. El código consiste en un máximo de 32 caracteres que la mayoría de las veces son alfanuméricos (aunque el estándar no lo específica, así que puede consistir en cualquier carácter). Todos los dispositivos inalámbricos que intentan comunicarse entre sí deben compartir el mismo SSID.

SSL	*(Secure Socket Layer)* Protocolo de capa de conexión segura. Proporciona autenticación (identidad) y privacidad de la información mediante el uso de criptografía.

stakeholder	Personas, accionistas empleados, clientes, grupo de personas o institución que se interesa por el buen funcionamiento de una empresa.

STP	*(Shielded Twisted Pair).* Par torcido blindado. Tipo de cable. El STP se define con un blindaje individual por cada par, más un blindaje que envuelve a todos los pares.

supply chain	Cadena de suministro. Hace referencia a la compleja serie de procesos de intercambio o flujo de materiales y de información que se establece tanto dentro de cada organización o empresa como fuera de ella, con sus respectivos proveedores y clientes.

TI	Tecnología(s) de Información

TIC	Tecnologías de Información y Comunicaciones (TIC)

TMN	*(Telecommunications Management Network)* Administración de Redes de Telecomunicaciones fue introducido por la ITU-T, y está definido en la reco-mendación M.3010. Aunque en un principio no hubo mucha colaboración entre los grupos de gestión de red de la ISO y el CCITT (germen de la ITU-T), posteriormente fueron incorporados varios conceptos del modelo OSI al estándar TMN.

transaccional	Una transacción es un evento o proceso que genera o modifica la infor-mación que se encuentra eventualmente almacenada en un sistema de información.

TSL	*(Transport Layer Security)* Seguridad de la capa de transporte. Evolución del protocolo SSL.

UNAM	Universidad Nacional Autónoma de México

URL	Localizador Uniforme de Recursos, son las siglas en inglés de U*niform Resource Llocator*. Se utiliza para nombrar recursos en Internet. Este nombre tiene un formato estándar y su propósito es asignar una dirección única a cada uno de los recursos disponibles en Internet, por ejemplo textos, imágenes, vídeos, etc.

USB	(*Universal Serial Bus*) Bus Universal en Serie o Conductor Universal en Serie (CUS), abreviado comúnmente USB, es un puerto o bus externo que provee capacidades para transferir datos a una velocidad de 12 Mbps y puede conectar hasta 127 dispositivos periféricos. Fue creado en 1996 por siete empresas (que actualmente forman el consejo directivo): IBM, Intel, Northern Telecom, Compaq, Microsoft, Digital Equipment Corporation y NEC. El diseño del USB tenía en mente eliminar la necesidad de adquirir tarjetas separadas para poner en los puertos bus ISA o PCI, y mejorar las capa-cidades *plug-and-play*, así como permitir a esos dispositivos ser conectados o desconectados al sistema sin tener que de reiniciar. Sin embargo, en aplicaciones donde se requiere ancho de banda para grandes transferencias de datos, una latencia baja, los buses PCI o PCIe salen ganando. Igualmente sucede si la aplicación necesita robustez industrial. A favor del bus USB, cabe decir que cuando se conecta un nuevo dispositivo, el servidor lo enumera y agrega el software adecuado para que pueda funcionar (esto dependerá ciertamente del sistema operativo que se esté usando).

UTP	*(Unshielded Twisted Pair)* Par torcido no blindado. Tipo de alambre. Es sin duda el que hasta ahora ha sido mejor aceptado, por su costo accesible y su fácil instalación.

v.g.	*Verbi gratia* es una locución latina de uso actual que significa "ejemplo" o "por ejemplo"; es muy utilizada con fines didácticos.

VLSI	*(Very Large Scale Integration)* Integración en escala muy grande.

VPN	Acrónimo de Virtual Private Network**.** Una red privada virtual, es una tecnología de red que permite una extensión segura de la red local sobre una red pública o no controlada como Internet. Ejemplos comunes son la posibilidad de conectar dos o más sucursales de una empresa utilizando como vínculo Internet, permitir a los miembros del equipo de soporte técnico la conexión desde su casa al centro de cómputo, o que un usuario pueda acceder a su equipo doméstico desde un sitio remoto, por ejemplo, un hotel. Todo ello utilizando la infraestructura de Internet.

War dialing o demon dialing	Es una técnica utilizada durante las décadas de 1980 y 1990, que consistía en hacer llamadas a una serie de números de teléfono en forma automática con el fin de encontrar módems conectados y permitiendo la conexión con algún otro equipo de cómputo.

Web	La palabra Web (del inglés: red, malla, telaraña) puede referirse a: *World Wide Web* (también conocida como 'la Web'), el sistema de documen-tos (o páginas web) interconectados por enlaces de hipertexto, disponibles en Internet. • World Wide Web, el primer navegador web, más tarde renombrado a Nexus. • Una página Web: documento o fuente de información, generalmente en formato HTML y que puede contener hiperenlaces a otras páginas Web. Dicha página Web, podrá ser accesible desde un dispositivo físico, una intranet, o Internet. • Un sitio Web, que es un conjunto de páginas Web, típicamente comunes a un dominio o subdominio en la World Wide Web. • Un servidor Web, un programa que implementa el protocolo HTTP para transferir lo que llamamos hipertextos, páginas web o páginas HTML. También se le da este nombre, al ordenador que ejecuta este programa. • Web 2.0, término acuñado por Tim O'Reilly en 2004 para referirse a una segunda generación de Web basada en comunidades de usuarios y una gama especial de servicios Web, como las redes sociales, los blogs, los wikis o las folcsonomías, que fomentan la colaboración y el intercambio ágil de información entre los usuarios. • Web 3.0: El término Web 3.0 apareció por primera vez en 2006 en un artículo de Jeffrey Zeldman, crítico de la Web 2.0 y asociado a tecnolo-gías como AJAX. Actualmente existe un debate considerable en torno a lo que significa Web 3.0, y cuál es la definición acertada.

WEP	*(Wired Equivalent Privacy)* es el sistema de cifrado incluido en el estándar IEEE 802.11. Este cifrado usa un algoritmo de 64 bits (existe ya de 128 bits) para revolver los paquetes de datos.

Wireless	Comunicación inalámbrica (*wireless*, sin cables) es aquella en la que extre-mos de la comunicación (emisor/receptor) no se encuentran unidos por un medio de propagación físico, sino que se utiliza la modulación de ondas electromagnéticas a través del espacio. En este sentido, los dispositivos físicos sólo están presentes en los emisores y receptores de la señal, entre los cuales encontramos: antenas, computadoras portátiles, PDA, teléfonos móviles, etc.

WS	*(Workflow Systems)* Sistemas de Flujo de Trabajo. El flujo de trabajo es el estudio de los aspectos operacionales de una actividad de trabajo: cómo se estructuran las tareas, cómo se realizan, cuál es su orden correlativo, cómo se sincronizan, cómo fluye la información que soporta las tareas y cómo se le hace seguimiento al cumplimiento de las tareas.

BIBLIOGRAFÍA

BIBLIOGRAFIA

Análisis y evaluación del riesgo de la información: caso de estudio Universidad Simón Bolívar, Vidalina De Freitas, *versión impresa* ISSN 1690-7515, Enlace v.6 n.1 Maracaibo abr. 2009.

Analytical Methods for Risk Management, Paul R. Garvey, CRC Press, 2009.

Artículo, Gestión de riesgos TI. Como implantar las mejores prácticas, Luis Fuertes, Marketing Manager de Symantec.

Auditoría en entidades de salud. Beltrán Pardo, Luís Carlos. Universidad Nacional de Colombia,http://www.virtual.unal.edu.co/cursos/economicas/91337/. Licencia: Creative Commons BY-NC-ND.

Comparte este artículo!, http://www.estrategiamagazine.com/tecnologia/sistema-de-informacion-y-tecnologia-de-la-informacion-ciencia-tecnica-it-is-ti-ntic-que-es-un-sistema-de-informacion-que-es-tecnologia-definicion-que-es-informatica-definicion/ (Consulta 13-11-2012).

Comparte este artículo!, http://www.estrategiamagazine.com/tecnologia/sistema-de-informacion-y-tecnologia-de-la-informacion-ciencia-tecnica-it-is-ti-ntic-que-es-un-sistema-de-informacion-que-es-tecnologia-definicion-que-es-informatica-definicion/ (Consulta 13-11-2012).

Contratos Informáticos Julio Téllez Valdes, Primera edición 1988. Universidad Nacional Autónoma de México, instituto de Investigaciones Jurídicas, C.U, 04510, México, D.F.

Cox, LA Jr.: '¿Qué hay de malo con matrices de riesgo?', Análisis de Riesgos, vol. 28, No. 2, 2008, doi : 10.1111/j.1539-6924.2008.01030.x

Del libro “Estrategia y sistemas de información” Andreu-Ricard-Valor, Editoral McGraw-Hill

Departamento Administrativo de la Función Pública, Departamento Administrativo de la Función Pública, República de Colombia, Bogotá, D.C., junio de 2004 Segunda Edición En prevención de riesgos de Chile, Editorial SIGWEB, 2010.

Dirección, organización y administración de centros de tecnología de información Coautores: Heriberto Olguín Romo. Editorial: Facultad de Ingeniería, UNAM, 2ª Edición Noviembre 2007

Estrategia competitiva, Michael E. Porter, Editorial Continental S.A. México 1997

Fundamentals of Enterprise Risk Management, John J. Hampton, AMACOM, 2009.

Gestión estratégica de seguridad en la empresa, GMV et al. Edición Anetcom. 2010.

Guía Avanzada de Gestión de Riesgos, LNCS, Instituto Nacional de Tecnologías de la Comunicación, Diciembre 2008.

http://protejete.wordpress.com/gdr_principal/matriz_riesgo/ (Consulta 10/12/2012).

http://www.isaca.org/COBIT/Documents/COBIT5-Framework-Spanish.pdf (Consulta: 10/07/2012).

http://www.segu-info.com.ar/ataques/ataques.htm (Consulta 10/12/2012).

http://www.sigweb.cl/biblioteca/MatrizdeRiesgo.pdf (Fecha de consulta 09/12/2012).

http://www.slideshare.net/profesorflavio8a/escenarios-de-riesgos (Consulta 09/12/2012).

Implementación programa administración del Riesgo, Escuela Superior de Administración Pùblica, Bogotá, D.C.Diciembre de 2006 Impreso y hecho en México ISBN 968-36-0619-9.

Ingeniería de Proyectos informáticos: actividades y procedimientos, José Salvador Sánchez Garreta, Ricardo Chalmeta Rosalen, Oscar Coltell Simon, Pilar Monfort Manero, cristina campos sancho. Biblioteca de la Universitat Jaume I. Dades catalográfiques.

Ingeniería del Software, Un Enfoque Práctico, Roger Pressman, Mc Graw hill 7ta Edición 2010.

Introducción a Riesgo Informático, Material Informático, Leonardo Sena y Simon Mario Tenzer, Agosto 2004.

ISACA. COBIT 5 Disponible en:
La revisión de los controles generales en un entorno informatizado, Antonio Minguillón Roy, Auditoría Pública nº 52 (2010).

MAGERIT - Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, http://www.csi.map.es/csi/pg5m20.htm

Manual de políticas y procedimientos de gestión de riesgos, Banchile corredores de bolsa S.A. 2009.

Manual Normativo de Riesgo Tecnológico, Coordinación de Riesgos-INFONAVIT, Octubre 2009.

Metodología de Análisis de Riesgo, Rodrigo Ferrer CISSP, SISTESEG, Bogota Colombia 2006.

Metodología y gobierno de la gestión de riesgos de tecnologías de la información, Ricardo Gómez y Diego Hernán Pérez, 31# Revista de Ingeniería, Agosto de 2010.

Normas Técnicas en Tecnologías de Información y Comunicaciones. Anexo NTP3.

OCTAVE, http://www.utpl.edu.ec/eccblog/wp-content/uploads/2007/04/articulo técnico evaluación de amenazas y vulnerabilidades de recursos criticos operacionales octave a nivel de usuario final para la utpl.pdf (Consulta 8/7/2012)

Outsourcing en Tecnologías de Información Coautores: Heriberto Olguín Romo, Ahedo, García, Hernández y Mancillas. Editorial: Facultad de Ingeniería, UNAM. 1ª Edición agosto 2007.

Principles of Information Security, Michael E. Whitman and Herbert J. Mattord, COURSE TECHNOLOGY, 2012.

Reingeniería de la Auditoría Informática Autor: Gustavo Adolfo Solís Montes, CISA; Editorial: Trillas, 1ª Edición marzo de 2002.

Riesgo Operativo XXIII Congreso AMA, ACT. Elvia Ojeda Apreza, Septiembre, 2007

Riesgos financieros y económicos, productos derivados y decisiones económicas bajo incertidumbre, Francisco Venegas Martínez, Segunda edición.

Riesgos financieros y operacionales internacionales, Diego Gómez Cáceres, Jesús miguel López Zaballos. ESIC EDITORIAL, ISBN: 84-7356-326-3.

Seguridad de la Información, Javier Areitio, Editorial PARANINFO 2008 CENGAGE Learning, ISBN: 978-84-9732-502-8

Sistemas de control interno para organizaciones, Oswaldo Fonseca Luna, coso.coco-basel-guia turnbull- COBIT-ERM-SOX-INTOSAI-OMB A-123, Primera Edición ISBN N° 978-9972-2948-3-9.

Tesis: “Administración de Riesgos de Tecnología de Información de una Empresa del Sector Informático”, Escuela superior politécnica del litoral, Instituto de Ciencias Matemáticas Auditoría y Control de Gestión, Año 2005.

The Basics of Information Security, Jason Andres, SYNCRESS, 2011

The Security Risk Assessment Handbook, Douglas J. Landoll, CRC Press Se, Second Edition, 2011.

Tratamiento de riesgos de seguridad, Universidad Nacional Federico Villarreal, 2011

Una metodología de ayuda para auditar Tecnologías de Información Autor: Heriberto Olguín Romo Editorial: Facultad de Ingeniería, UNAM, 1ª Edición Diciembre de 2011.