UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

PROGRAMA DE MAESTRÍA Y DOCTORADO EN INGENIERÍA
INGENIERÍA EN SISTEMAS - INVESTIGACIÓN DE OPERACIONES

METODOLOGÍA PARA LA MODELACIÓN Y TRATAMIENTO DE RIESGOS INFORMÁTICOS USANDO HERRAMIENTAS COMBINADAS DE INVESTIGACIÓN DE OPERACIONES

TESIS
QUE PARA OPTAR POR EL GRADO DE:
MAESTRO EN INGENIERÍA

PRESENTA:
ISRAEL ANDRADE CANALES

TUTOR PRINCIPAL:
JUAN MANUEL ESTRADA MEDINA, FACULTAD DE INGENIERÍA

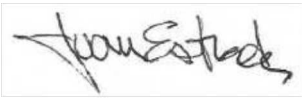
MÉXICO D.F. ENERO 2014

JURADO ASIGNADO:

Presidente:	IDALIA FLORES DE LA MOTA
Secretario:	FRANCISCA IRENE SOLER ANGUIANO
Vocal:	JUAN MANUEL ESTRADA MEDINA
1^{er} Suplente:	ANN GODELIEVE WELLENS PURNAL
2^{do} Suplente:	ESTHER SEGURA PÉREZ

Lugar donde se realizó la tesis:
FACULTAD DE INGENIERÍA, UNAM

TUTOR DE TESIS:
JUAN MANUEL ESTRADA MEDINA



FIRMA

Agradecimientos

El siguiente escrito representa mi segunda aportación de ideas que tienen como objetivo tomar la responsabilidad de fortalecer la cultura y la investigación para crear un mejor país; responsabilidad que me ha inculcado la Universidad Nacional Autónoma de México. Sin embargo, este esfuerzo se ha visto iluminado por mis padres: Hilda y Javier; mis hermanos: Ismael, Karina y Javier; mi hija Quetzalli; Elizabeth y mis amigos: Ricardo, Alex, Adriana, entre otros que no incluyo porque el margen de esta página es demasiado estrecho.

Agradezco de manera especial a mi tutor el Dr. Juan Manuel Estrada Medina y a la Dra. Idalia Flores de la Mota quienes durante la elaboración de este trabajo me brindaron su apoyo en la investigación. Gracias a mis sinodales: la Dra. Esther Segura, la M. I. Ann Wellens y la M. I. Francis Soler, porque cada uno de sus comentarios enriquecieron esta tesis.

Además, agradezco al Consejo Nacional de Ciencia y Tecnología (CONACYT) por el financiamiento otorgado durante la maestría.

Israel Andrade Canales

Tabla de contenido

Introducción

Actualmente, la información es un activo de gran valor que es utilizado por personas y organizaciones para la toma de decisiones, comunicar ideas y generar conocimiento; además, es indispensable en el ámbito laboral para el ofrecimiento de servicios y la creación de productos. En este sentido, la sociedad ha generado conciencia de la importancia de la información en su vida diaria, y por ello se ha considerado así misma como la sociedad de la información. Debido a esta relevancia, también se han desarrollado tecnologías llamadas "Tecnologías de la Información y Comunicación" que facilitan su procesamiento, almacenamiento y transmisión.

Sin embargo, existen algunos factores que afectan la integridad, confidencialidad y disponibilidad este valioso recurso; por ejemplo, las deficiencias en el diseño de las tecnologías que procesan la información, y los hábitos perjudiciales que tienen los usuarios de dicho activo. Lo anterior ha generado problemas de seguridad que afectan a usuarios y organizaciones en el logro de sus objetivos.

Es por esto que la seguridad informática es un área de estudio en crecimiento que en las últimas décadas ha tomado una atención destacada. Inicialmente, esta disciplina sólo se enfocaba en la solución de los problemas técnicos que ocasionan los problemas de seguridad, pero en los últimos años esta área ha utilizado diferentes estrategias para enfrentar una problemática que involucra no sólo aspectos computacionales, también aspectos legales y humanos. En particular, el estudio del riesgo informático se ha vuelto una estrategia destacada donde se han utilizado técnicas de diferentes áreas de estudio para el análisis de los elementos que ocasionan los incidentes informáticos. En general, existen dos enfoques para llevar a cabo una evaluación del riesgos: a través de metodologías cualitativas y cuantitativas.

Las metodologías cualitativas utilizan principalmente el conocimiento de los expertos en la materia para efectuar el análisis de riesgos; estas son útiles

cuando no se cuenta con los datos suficientes para realizar un modelo preciso basado en datos históricos, y suelen ser más sencillas de implementar; sin embargo, no ofrecen herramientas exactas para la realización de pronósticos.

Por otro lado, las metodologías cuantitativas están basadas en modelos que analizan los datos de registros de incidentes informáticos previos; estas ofrecen información más precisa para la toma de decisiones; en contraste, son difíciles de implementar debido a la cantidad de datos que se requieren para llevarse a cabo; además, estas metodologías se encuentran como trabajos aislados dentro del área, sin combinar los diversos beneficios que pueden aportar.

Por lo anterior, en el presente trabajo se propone una metodología cuantitativa para el análisis y tratamiento de riesgos informáticos que combina dos herramientas matemáticas que, por una parte, facilitan el análisis del riesgo, y por otra, apoya en la gestión del mismo. Estos dos aspectos son fundamentales en la mitigación efectiva del riesgo y actualmente las metodologías cuantitativas no tratan en conjunto. Por otro lado, pretende ser una herramienta útil una vez que se ha trabajado con metodologías cualitativas, y de esta manera obtener resultados más objetivos basados en los incidentes previamente registrados.

Objetivo

El objetivo general de la investigación es proponer una metodología cuantitativa que combina la simulación y la programación entera para analizar y tratar eficientemente el riesgo informático a través del estudio de los incidentes informáticos registrados.

Los objetivos específicos de este trabajo son:

- Realizar una revisión bibliográfica del estado del arte de las metodologías de análisis del riesgo informático y discutir las diferentes características de las más representativas.
- Revisar las herramientas de investigación de operaciones más adecuadas para el análisis y tratamiento de incidentes informáticos y proponer una metodología que las integre.
- Caracterizar el comportamiento de los incidentes informáticos reportados en una entidad académica desde un enfoque estadístico para estimar y

explorar escenarios adversos de incidentes informáticos en un caso de estudio.

- Proponer un plan de tratamiento de riesgos factible y eficiente.
- Evaluar la efectividad de esta metodología desarrollada a través de una prueba estadística.

Alcance y limitaciones

Debido a que la metodología de análisis de riesgos propuesta en este trabajo es cuantitativa, es necesario contar con un registro de incidentes informáticos suficiente para construir los modelos matemáticos que aquí se presentan; por lo tanto, se sugiere que esta metodología se implemente cuando se tenga un sistema de reporte de incidentes operando; por otro lado, la organización debe tener una forma de medir el impacto de los incidentes informáticos en términos monetarios, productividad, reputación, etc. Por lo tanto, esta metodología debe llevarse a cabo junto con los expertos de seguridad de la organización. Una observación importante en este sentido es que esta metodología es adecuada en la transición entre una metodología cualitativa a una cuantitativa.

Estructura de la tesis

Para poner en contexto lo mencionado anteriormente, en el primer capítulo de esta tesis se presentan algunos aspectos fundamentales de la problemática de la seguridad de la información, conceptos relacionados con este tema, así como el estado del arte de las metodologías de análisis y tratamiento de riesgos.

En el segundo capítulo se presenta la metodología de análisis de riesgos así como el marco conceptual de las herramientas utilizadas en ella. Aquí se ofrece una explicación de los conceptos importantes de las herramientas de simulación y programación entera. En el capítulo 3, se presenta el caso de estudio utilizado para la evaluación de la metodología así como el desarrollo del análisis de riesgos que propone el presente trabajo; principalmente prestando interés en la técnica de simulación aplicada en la estimación de incidentes informáticos y sus resultados. El cuarto capítulo detalla la segunda parte de la metodología

propuesta, particularmente en el modelo de optimización para el tratamiento del riesgo y los resultados obtenidos.

Finalmente, la última sección del trabajo menciona las conclusiones, las cuales, también ofrecen recomendaciones sobre los posibles trabajos y futuras líneas de investigación.

Capítulo 1

El problema de la seguridad de la información

En este capítulo se hace una breve exposición sobre la problemática asociada con la seguridad de la información y el estado del arte de los enfoques utilizados para afrontar dicha cuestión. Lo anterior con el fin de ubicar y destacar las aportaciones que presenta este trabajo.

La seguridad informática es un tema que toma importancia conforme se incrementa el uso de las tecnologías de la información (TI) en la vida cotidiana; para ilustrar lo anterior, véase la nota que publicó el periódico mexicano La Jornada (Aranda, 2013) en la primera plana del día 17 de enero de 2013 (Figura 1.1), en la cual se narra el ataque informático que sufrió la Secretaría de la Defensa Nacional (Sedena) por parte de un colectivo de hacktivistas[1] llamado Anonymous Hispano, que aseguraron haber modificado el contenido del sitio web del ejército, además de haber robado «por completo toda su información», advirtiendo también que harían pública dicha información en fechas próximas.

Este suceso no sólo afectó por algunas horas la disponibilidad de la información pública que ofrece la Sedena en su página de internet, también afectó su reputación y credibilidad en materia de seguridad. Cabe destacar que esto es sólo un ejemplo de este tipo de sucesos; sin embargo, estos incidentes ocurren con frecuencia en distintas organizaciones de todo el mundo.

[1]Hacktivista es la unión de las palabras «Hacker» y «Activista» la cual se refiere a un intruso informático que realiza protestas políticas y sociales.

La Jornada

DIRECTORA GENERAL: CARMEN LIRA SAADE
DIRECTOR FUNDADOR: CARLOS PAYAN VELVER

JUEVES 17 DE ENERO DE 2013
MÉXICO, DISTRITO FEDERAL • AÑO 29 • NÚMERO 10218 • www.jornada.unam.mx
10 PESOS

■ El colectivo Anonymous lanzó al menos tres ataques; el portal de Marina, también afectado

www.sedena.gob.mx

Kicking Your Ass Since 2011 twitter: @Anon_Centr | #AnonymousMexi

Al pueblo de México,A los pueblos y gobiernos del mundo.

Hermanos:

Nosotros nacimos de la noche. En ella vivimos. Moriremos en ella. Pero la luz será mañana para los mar, para todos aquellos que hoy lloran la noche, para quienes se niega el día, para quienes es regalo la muerte, para quienes está prohibida la vida, para todos la luz. Para todos todo. Para nosotros el dolor y la angustia,

En el portal de la Secretaría de la Defensa Naciona una voz en *off* leía lo que llamó el *Manifiesto Zapatista Anonymus*, mientras se veían imágenes de los hechos violentos ocurridos durante la toma de posesión de Enrique Peña Nieto y escenas de la película *El gran dictador*, de Charles Chaplin. El sitio sufrió el primer ataque a las 14 horas, luego a las 15 y finalmente a las 18:25 horas

Queda fuera la página web de Sedena tras ser *hackeada*

■ Los piratas cibernéticos dijeron que "robaron" toda la información del Ejército

■ "Nuestra red interna funciona con normalidad", apuntan fuerzas armadas

Jesús Aranda ■ 3

Confirman el auto de formal prisión a tres generales

■ Fallidas apelaciones de Tomás Ángeles, Roberto Dawe y Rubén Pérez

■ Magistrada da sustento a las aseveraciones que los ligan con los Beltrán

Figura 1.1: Portada del periódico La Jornada el día 17 de enero de 2013

De acuerdo con la encuesta Information security branches (PWC, 2012) en 2012 nueve de cada diez grandes empresas en el Reino Unido registraron un evento de seguridad cuyo costo fue entre 110 a 250 mil libras. Estos incidentes informáticos fueron generados por diversas causas: principalmente por fallas en la infraestructura, eventos provocados por el personal interno y ataques provocados por gente no autorizada.

Otro ejemplo son las cifras que la Universidad Nacional Autónoma de México ha publicado en materia de incidentes informáticos (Figura 1.2). La UNAM ha reportado un número mayor de este tipo de sucesos dentro de su red interna en los últimos 8 años de acuerdo con las estadísticas publicadas por el equipo de respuesta a incidentes informáticos de esta organización UNAM-CERT (UNAM-CERT, 2012). Estos datos muestran que los percances informáticos han incrementado considerablemente de 2004 a la fecha estabilizándose en los últimos 2 años. Estos sucesos informáticos no sólo afectan la infraestructura de cómputo provocando que estos recursos sean utilizados de maneras no autorizadas, además ponen en riesgo la información con la que la universidad logra sus objetivos.

Figura 1.2: Incidentes registrados en Red UNAM de 2004 a 2012. La organización reportó que el pico ocurrido durante 2009 sucedió debido al cambio configuraciones en los sensores que detectaron dichos eventos.

1.1. Incidentes informáticos

Un incidente informático es uno o varios eventos inesperados que tienen una probabilidad significativa de comprometer las operaciones de una organización y amenazar la seguridad informática (ISO/IEC, 2009). Estos percances perjudican a los activos de información provocando pérdidas de algún tipo a sus propietarios; por ejemplo: pérdidas económicas, tiempos de operación desperdiciados, falta de credibilidad o reputación, etc. Sin embargo, aunque los incidentes informáticos afectan a las organizaciones de diferente manera, ellos presentan características similares que es posible analizar ya que estos sucesos se presentan cuando existen dos elementos importantes: las vulnerabilidades y las amenazas.

1.1.1. Vulnerabilidades

Una vulnerabilidad es una debilidad en la infraestructura tecnológica o en un control de seguridad que puede ser aprovechada por una amenaza (ISO/IEC, 2009). En el contexto informático, las vulnerabilidades más frecuentes son los

errores en el diseño y programación de software. Esto ocurre porque comúnmente no se hacen pruebas exhaustivas de fallas, provocando de esta manera que dichos programas informáticos se comporten de manera inesperada.

Otro tipo de vulnerabilidad es la falta de políticas y procedimientos en el manejo de la información confidencial; consecuentemente, dicha información puede ser accedida por cualquier persona no autorizada y emplearse de manera inadecuada. Del mismo modo, la falta de mantenimiento a la infraestructura de cómputo es otro tipo de vulnerabilidad que frecuentemente ocurre, la cual ocasiona que el hardware genere fallos inesperadamente y pone en riesgo la integridad de la información.

1.1.2. Amenazas

El otro factor que interviene en los incidentes informáticos son las amenazas. Las amenazas son elementos que tienen el potencial de provocar un evento que puede generar un daño a la organización (ISO/IEC, 2009). Algunos ejemplos de amenazas en el campo de la informática son: los programas maliciosos (también conocidos como malware), los intrusos (llamados comúnmente hackers), los desastres naturales, entre otros. Cabe destacar que estos elementos pueden ser generadas por causas naturales y humanas. Estas últimas pueden ser provocadas de manera deliberada o accidental. La figura 1.3 ilustra la naturaleza de las amenazas informáticas.

1.1.3. Riesgos informáticos

Las vulnerabilidades como las amenazas siempre están presentes en cualquier esquema informático; en otras palabras, siempre existe la probabilidad de que una vulnerabilidad sea explotada por una amenaza y se afecte así la información. Cuando existe esta probabilidad, existe un riesgo a la información. Por lo tanto el riesgo son eventos, que si ocurren, causarían un costo adverso a los costos, productividad y desempeño de una organización(Garvey, 2009). Otras fuentes como el ISO 27000 lo definen como la combinación de un evento (en este caso un incidente informático) y su consecuencia(ISO/IEC, 2009). Por tal motivo, los dueños de la información tienen como objetivo mitigar estos percances utilizando contra-medidas o controles que reducen la probabilidad de que ocurran los incidentes, o bien, disminuyen el daño que ocasionan.

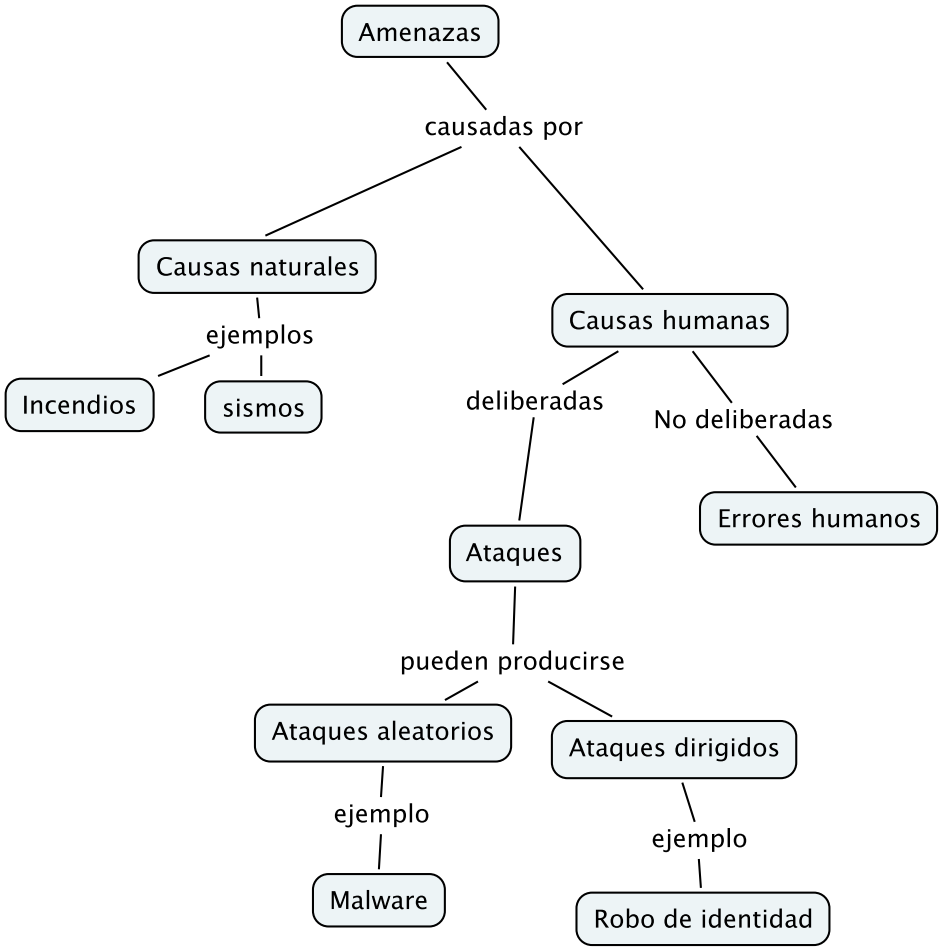


Figura 1.3: Mapa conceptual de la naturaleza de las amenazas informáticas. *Fuente: elaboración propia a partir de los conceptos tomados de (Pfleeger and Pfleeger, 2003)*

1.1.4. Controles de seguridad

Considerando esta situación, durante las últimas décadas se han desarrollado mecanismos o contra-medidas que tienen la tarea de reducir los riesgos informáticos. Estos controles son acciones, dispositivos, procedimientos o técnicas que reducen las vulnerabilidades y minimizan el daño que dichos sucesos provocan (Pfleeger and Pfleeger, 2003).

Un control es un medio para modificar un riesgo informático incluyendo políticas, procedimientos, guías y prácticas organizacionales; los cuales pueden ser de tipo administrativo, técnico o legal. Es decir, en la reducción de los riesgos informáticos no sólo intervienen factores tecnológicos como dispositivos de red, antivirus y algunas herramientas matemáticas como la criptografía; también intervienen factores humanos como leyes y procedimientos.

Los conceptos mencionados anteriormente están estrechamente relacionados. El análisis de la seguridad informática a través de estas relaciones se conoce como el paradigma amenaza-vulnerabilidad-control (Buchanan, 2011). La figura 1.4 muestra un mapa conceptual con las relaciones que existen entre los conceptos previos. En el diagrama se muestra que los elementos principales que intervienen en los riesgos informáticos son las amenazas y las vulnerabilidades; en el mismo diagrama, los incidentes informáticos son los riesgos que se materializaron y que afectan a los activos de información; siendo los controles de seguridad, el principal mecanismo para atenuar sus efectos.

1.2. Estrategias de seguridad informática basadas en riesgos

Las amenazas y las vulnerabilidades son los principales elementos que provocan los incidentes informáticos. Estos sucesos provocan daños a las organizaciones y a los usuarios al comprometer la a seguridad de la información; para evitar lo anterior, la estrategia más común es implementar controles de seguridad para atenuar los efectos de dichos percances; por ejemplo, si se detectan intrusiones dentro de una red informática, lo más común es que se instale un equipo para bloquear dicha intromisión. Sin embargo, actualmente existen diferentes tipos de amenazas y vulnerabilidades que pueden afectar a una organización, y cada una de ellas puede provocar daños a diferentes escalas. Por lo tanto, es necesario diseñar un plan para mitigar los riesgos más peligrosos dentro de

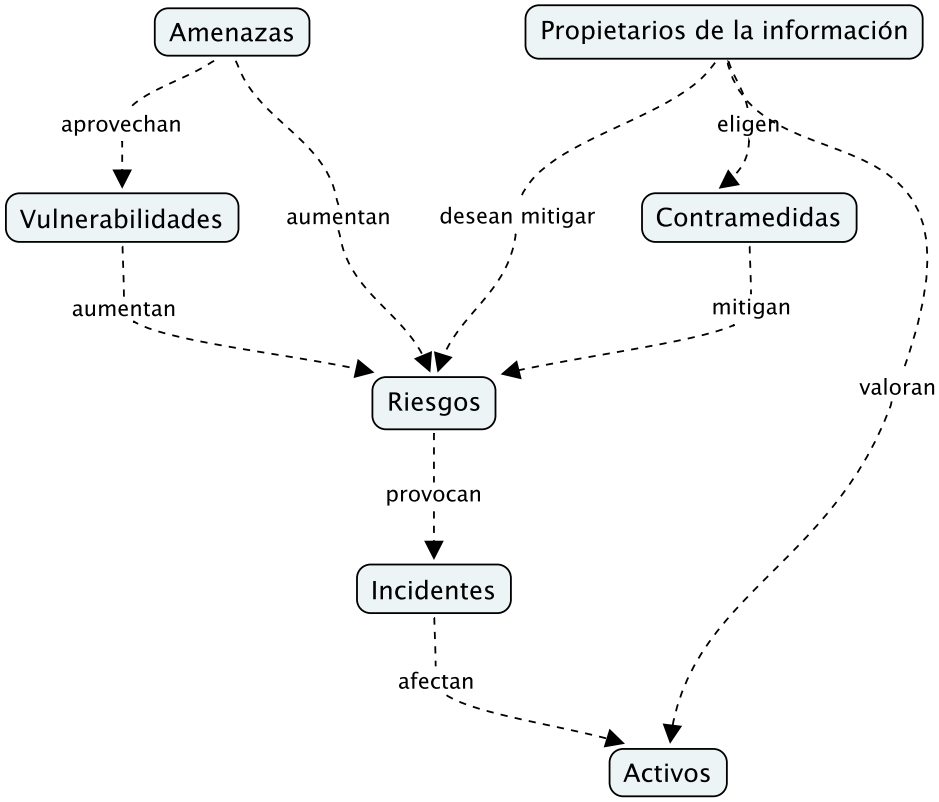


Figura 1.4: Mapa conceptual de incidentes informáticos. *Fuente: elaboración propia a partir de los conceptos tomados de (Pfleeger and Pfleeger, 2003)*

una organización considerando su costo; y para ello, existen diferentes tipos de herramientas entre las que destacan el análisis de riesgos y las metodologías para su tratamiento.

El análisis y tratamiento del riesgo son dos actividades importantes para mejorar el estado de seguridad en cualquier organización. Sin embargo, existen diferente maneras de realizar estas actividades. En la siguiente sección se analiza el estado del arte de las metodologías de análisis de riesgos así como el de su tratamiento.

1.2.1. Análisis de riesgos informáticos

El análisis de riesgos es un método para analizar las relaciones que existen entre amenazas, vulnerabilidades y los daños que pueden ocasionar a la confidencialidad, integridad y disponibilidad de la información. En general, en el análisis de riesgos se identifican las amenazas y vulnerabilidad más importantes, se determina cual es la probabilidad de que ocurra un incidente dado estos factores y se estima el impacto o daño de estos percances.

Para llevar a cabo dicho análisis, se utilizan distintos tipos de fuentes de datos tales como estadísticas de incidentes, bitácoras de sucesos, etc (ISO/IEC, 2009). Las metodologías de riesgos utilizan diversos tipos de técnicas para evaluar dichos datos. En general, se pueden clasificar estas metodologías en dos tipos distintos: por un lado las metodologías cualitativas, y por otro, las metodologías cuantitativas.

Las metodologías cualitativas tienen la característica de analizar el riesgo a través de la información que ofrecen los expertos en materia tecnológica y en la información que brindan los dueños de los activos. Además, la información está dada en forma categórica; es decir, en vez de manejarse números se utilizan etiquetas con diferentes jerarquías; por ejemplo, el valor de los activos puede establecerse como: «Crítico», «Importante» y «No importante»; la probabilidad de que ocurra un evento adverso a la seguridad puede etiquetarse como: «Muy probable», «Probable» o «Poco probable», etc (Gollman, 2011).

Por otro lado, las metodologías cuantitativas utilizan el análisis y la evaluación de datos a través de fuentes cuantitativas como estadísticas, bitácoras, etc. En adición, estas metodologías se basan en modelos matemáticos como la simulación (Winkelvos et al., 2011), los árboles de decisión (Sahinoglu, 2005) y las redes bayesianas. La ventaja principal es que al utilizar este tipo de fuente

de datos, las probabilidades calculadas por estas metodologías son más precisas. Sin embargo, se debe contar con datos de entrada precisos para llevarlas a cabo; de lo contrario,la calidad de los resultados obtenidos no será mejor que la calidad de los datos de entrada (Gollman, 2011).

En efecto, es necesario elegir la metodología de riesgos adecuada según las condiciones del problema, pues cada una de ellas ofrecerá ventajas y desventajas. Con el fin de analizar este último punto a continuación se presentan brevemente algunas metodologías de análisis de riesgos.

1.2.1.1. OCTAVE Allegro

OCTAVE Allegro (evaluación de amenazas, activos y vulnerabilidades operativas críticas, por sus siglas en inglés) es una metodología cualitativa cuya principal ventaja es que puede llevarse a cabo no sólo cuando existen datos insuficientes para hacer un análisis estadístico, también cuando los datos de entrada son subjetivos. Esta metodología cuenta con un conjunto de cuestionarios, formatos y diagramas que facilitan la obtención de información a partir de entrevistas a los expertos de la organización y la elaboración de «checklists». Sin embargo, esta metodología carece de una base estadística que pueda dar más precisión a los resultados; ya que el cálculo de la probabilidad de los incidentes no es obligatoria para llevarse a cabo (Software Engineering Institute, 2012). Por lo que esta metodología es útil para generar una concepción general del riesgo informático en la organización en las primeras etapas del análisis de riesgos.

1.2.1.2. Metodología de análisis de riesgos por simulación de Winkelvos et al.

La metodología de análisis de riesgos propuesta por Winkelvos et al. (Winkelvos et al., 2011) Es una metodología cuantitativa que utiliza como herramienta la simulación para identificar cual es el punto más débil en una estructura de cómputo. Para llevarla a cabo, se requiere establecer una red de cómputo e identificar las vulnerabilidades de cada equipo; de esta manera, se ponderan cada uno de las vulnerabilidades encontradas y un autómata decide que ruta de ataque seguiría un intruso. La principal ventaja de este trabajo es como realizar diferentes escenarios de interés para el analista de riesgos. Y el autómata que utilizó permite automatizar la evaluación de los diferentes escenarios. Esta

característica es destacable porque si la infraestructura de cómputo cambia, es posible calcular el riesgo de manera automática. Por otro lado, esta metodología no define claramente como analizar un riesgo procedente de una fuente no tecnológica, pues sólo se enfoca en las vulnerabilidades de los equipos. De esta manera, esta metodología es útil sólo para generar una conjetura de qué ruta utilizaría un intruso para realizar un ataque.

1.2.1.3. Metodología de análisis de riesgo basada en árboles de decisión de Sahinoglu

El modelo publicado por Sahinoglu en la revista IEEE Security and Privacy en 2005 (Sahinoglu, 2005) propone el uso de árboles de decisión para el análisis del riesgo. Los árboles de decisión son modelos de predicción que utilizan datos probabilísticos así como datos determinísticos para inferir las posibles utilidades o pérdida de acuerdo con las decisiones establecidas en una estructura ramificada llamada árbol. Por lo tanto, este tipo de herramientas puede ser utilizada para calcular el costo total de un incidente informático. En particular este modelo es útil para estimar el impacto de todos los incidentes tecnológicos así como los riesgos residuales; los cuales son el riesgo que sobra después de aplicar los controles de seguridad Sin embargo, sólo se enfoca en el aspecto tecnológico, y no brinda herramientas para integrarse a una metodología de tratamiento de riesgos.

1.2.2. Tratamiento de riesgos informáticos

El tratamiento del riesgo es un conjunto de actividades en las que se aplican controles de seguridad para disminuir la probabilidad de que ocurra un incidente informático (ISO/IEC, 2009). Sin embargo, la elección de controles de seguridad está sujeta a los presupuestos dedicados a la seguridad informática; al tiempo que se disponga para tratar los riesgos informáticos; al personal disponible para implementar dichos controles, etc.

En la actualidad, existen diferentes marcos de trabajo que cuentan con este enfoque, uno de los más conocidos es el enfoque utilizado en el modelo llamado «Sistema de gestión de seguridad de la información» propuesto por el estándar ISO 27001:2005 (ISO/IEC, 2005a). Por otro lado, la universidad Carnegie Mellon reportó un modelo que considera los recursos de la organización con el fin de invertir en la seguridad eficientemente. A continuación se mencio-

nan brevemente tanto el SGSI como el tratamiento de riesgos para presupuestos limitados.

1.2.2.1. Sistema de gestión de seguridad de la información

El estándar ISO 27001:2005 es una norma internacional que señala los requerimientos para implementar en cualquier tipo de organización una estrategia de seguridad llamada Sistema de gestión de seguridad de la información. Este sistema es un conjunto de actividades que tienen como objetivo la mejora continua del estado de seguridad de la información basándose principalmente en modelos de calidad, tales como el ciclo de Deming. Las actividades más importantes que se realizan en cada ciclo son el análisis de riesgos y el plan de tratamiento de riesgos.

El estándar no establece una metodología en particular para la actividad de análisis de riesgos; sin embargo, requiere que esta sea documentada y que sea repetible. Por otro lado, la metodología para tratar el riesgo identificado consiste en elegir un conjunto de controles de seguridad sugeridos en el anexo A de dicho documento. A pesar de que el conjunto de controles sugeridos por el estándar fue diseñado por expertos en seguridad, la metodología no menciona algún plan para la selección de controles de manera factible u óptima, por lo que puede ser complementada con otras metodologías que tengan dicho enfoque.

1.2.2.2. Tratamiento de riesgos informáticos para presupuestos fijos

Otro de los modelos que se revisó fue el tratamiento de riesgos para presupuestos fijos. De acuerdo con Caulkins et al. (Caulkins et al., 2007) se formuló un modelo matemático para la elección de controles de seguridad para la prevención de incidentes de seguridad basado en un modelo de programación entera que permite obtener una combinación factible y eficiente. Esta característica resulta importante al momento de elegir un plan de tratamiento de riesgos basado en un presupuesto fijo. Dicho reporte también mencionó su aplicación en un caso de estudio el cual se describe brevemente a continuación:

1. En el caso de estudio se propuse un presupuesto fijo para invertir en el tratamiento de riesgos
2. Para prevenir los incidentes de seguridad, en el estudio se utilizó una combinación de controles de seguridad administrativos (CA) y controles

técnicos (CT), donde el costo de prevenir un incidente es igual a la suma de todos los controles (CT y CA) calculados anualmente.

3. Cada incidente de seguridad se consideró como un parámetro binario y analizado bajo un modelo de programación entera.

4. Finalmente, cada control de seguridad posee un costo.

El estudio realizado donde se aplicó el modelo reportó que: El aumento de presupuesto no necesariamente implica la prevención de más incidentes. Nótese en la Figura 1.5 que para el rango de presupuestos de 0k - 40k no hay una mejora significativa en el número de incidentes prevenidos a pesar del aumento en el gasto. Estos resultados resaltan la importancia de un enfoque de optimización en el momento de realizar un plan de tratamiento de riesgos para destinar los recursos de seguridad eficientemente.

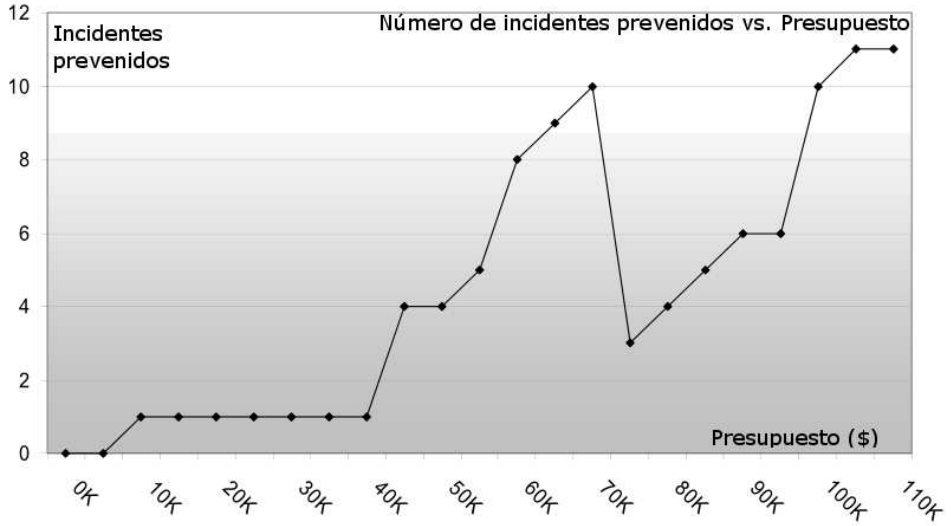


Figura 1.5: Gráfica de mitigación de incidentes de acuerdo con el presupuesto invertido. *Fuente: (Caulkins et al., 2007)*

Resumen

En este capítulo se discutió de manera somera la problemática de la seguridad de la información. Esta se debe principalmente a la interacción de amenazas,

vulnerabilidades y contra-medidas en los sistemas informáticos. Sin embargo, se han formulado diferentes estrategias para contrarrestar los daños que ocasionan los incidentes informáticos, donde los modelos más importantes son aquellos que se basan en el análisis del riesgo. Aunado a esto, existen diferentes tipos de metodologías de análisis de riesgos que principalmente se basan en métodos cuantitativos y métodos cualitativos. Por una parte los métodos cuantitativos utilizan herramientas matemáticas como la simulación y los árboles de decisión; por la otra, los métodos cualitativos utilizan información derivada de la experiencia de los analistas.

Por otra parte, se discutieron dos metodologías para el tratamiento del riesgo. La primera se basa en modelos tomados de las áreas de calidad, las cuales aportan facilitan la gestión del riesgo; sin embargo, también se destacó la importancia de contar con un enfoque eficiente en este proceso de gestión para invertir adecuadamente los recursos destinados a la seguridad.

Capítulo 2

Análisis y tratamiento de riesgos informáticos

En este capítulo se describe la metodología desarrollada para el análisis y tratamiento de riesgos; para lo cual, primero se discuten los conceptos de simulación y programación entera, ya que estas herramientas fueron utilizadas en los modelos de simulación y optimización de la metodología. Durante dicha discusión, también se mencionan algunas ventajas que motivaron su utilización.

Por otro lado, en esta capítulo se detallan las fases de la metodología de análisis de riesgos que se propone en este trabajo. Esta metodología se divide en dos bloques principales: el análisis y el tratamiento de riesgos. El primer bloque corresponde al análisis de incidentes informáticos a través de la simulación, y el segundo bloque al tratamiento de riesgos a través de programación entera binaria.

2.1. Simulación

Los incidentes informáticos son fenómenos complejos ya que en ellos intervienen elementos como las amenazas, las vulnerabilidades y los controles de seguridad; estos elementos modifican la probabilidad de que los incidentes ocurran, así como impacto o daño que generan en de las organizaciones. Por lo tanto, un modelo de predicción preciso sería no factible o demasiado complejo para los algoritmos actuales de solución. Cuando un problema presenta estas características, es posible representarlo a través de modelos que tienen el obje-

tivo de «imitar» el comportamiento del sistema real; es decir, con modelos de simulación (Taha, 2011).

La simulación es un método numérico que permite imitar el comportamiento de un fenómeno de la vida real. Este involucra la formulación de un modelo que genera datos artificialmente. El análisis de dichos datos permite obtener inferencias sobre las características del fenómeno estudiado (Banks, 1998). Lo anterior, por un lado, permite la experimentación de escenarios a través de la simulación, y por otro, infiere que el método no sea un método exacto.

La experimentación de escenarios es una de las cualidades sobresalientes de la simulación; esta permite probar cambios dentro de un sistema sin la necesidad de alterarlo en la realidad. Por ejemplo, una organización puede manipular su proceso de producción en un modelo de simulación sin alterarlo físicamente. Otro ejemplo es la capacidad de alterar virtualmente el tiempo en el modelo para visualizar eventos del sistema (Banks, 1998). Aunado a esto, la experimentación de escenarios facilita conocer el comportamiento del sistema bajo condiciones extremas; por ejemplo, conocer la carga total de operaciones que permite un sistema antes de desestabilizarse, etc.

Sin embargo, la simulación no es un método exacto, ya que opera con datos artificiales; es decir, que los resultados de la simulación están sujetos a números aleatorios (Taha, 2011); por lo tanto, la simulación no puede ser utilizada como una técnica de optimización por sí misma. Lo anterior, también provoca que la interpretación de datos de la simulación sea una tarea complicada, ya que los datos pueden, por un lado, brindar información sobre el sistema real, o por el contrario, brindar datos no significativos (Banks, 1998).

En efecto, la simulación es una herramienta flexible y muy importante para analizar fenómenos complejos. Permite el análisis del sistema real a través de un modelo que puede ser manipulado para su experimentación. Sin embargo los modelos de simulación pueden ser inapropiados cuando un modelo analítico es preferible; en particular, porque los modelos de la simulación operan con variables aleatorias. Por lo anterior, es necesario saber que tipo de simulación es adecuada de acuerdo con la naturaleza del sistema estudiado. En general existen dos tipos de simulación: la simulación de sistemas continuos y la simulación de eventos discretos.

2.1.1. Simulación de sistemas continuos

Los modelos de simulación continuos utilizan variables que cambian continuamente a través del tiempo. Estas variables representan el estado del sistema y se definen generalmente por medio de (Banks, 1998):

- funciones explícitas ej. $y = f(x, t)$,
- funciones recursivas ej. $y_{n+1} = ay_n + bu_n$,
- ecuaciones diferenciales ej. $dy/dt = f(x, t)$.

Los resultados en este tipo de modelos se obtienen de calcular los valores de las variables de estado (las variables dependientes) a través de diferentes puntos en el tiempo (la variable independiente). Por ejemplo, si el sistema de interés es un avión en vuelo; una variable de estado es su posición actual, y este dato cambia continuamente con el tiempo.

2.1.2. Simulación de eventos discretos

Los modelos de simulación de eventos discretos son aquellos cuyas variables dependientes cambian únicamente en distintos puntos del tiempo simulado; por ejemplo, la llegada de un cliente a una terminal de servicio, la llegada de material a una máquina de producción, etc.

Para realizar un modelo de simulación con estas características no existe una metodología bien definida. Sin embargo, existen pasos fundamentales en el momento de su formulación. La Figura 2.1 ejemplifica las fases principales en el desarrollo de un modelo de simulación.

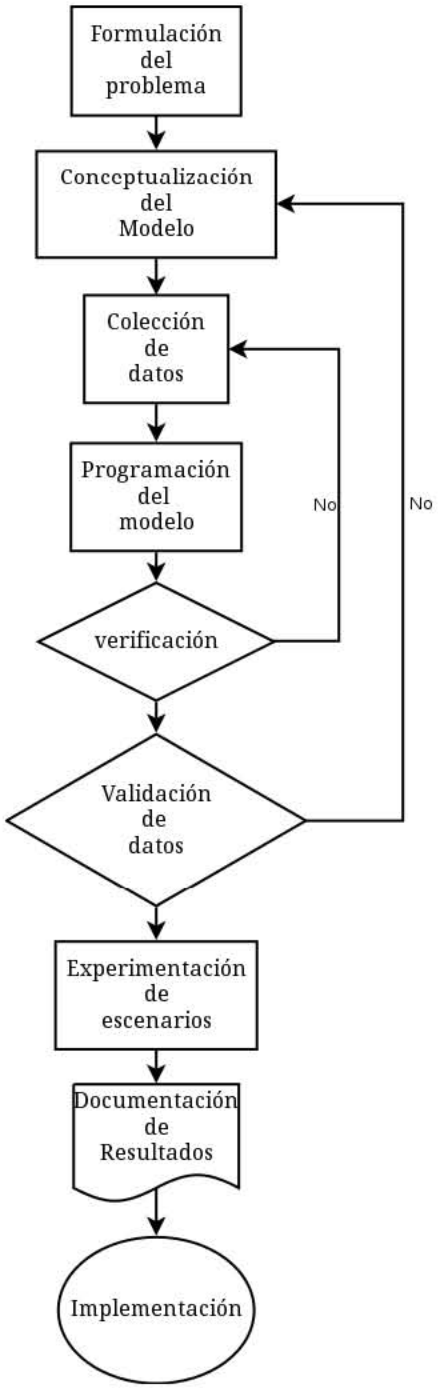


Figura 2.1: Diagrama de flujo del proceso de simulación basado en el modelo de Jerry Banks (Banks, 1998)

A continuación se enumeran algunas fases en el desarrollo de un modelo de simulación:

1. Formulación del problema: cada estudio de simulación empieza con la formulación detallada del problema que se desea enfrentar. Así como la identificación clara de los objetivos del estudio.

2. Conceptualización del modelo: En esta fase es necesario identificar las relaciones lógicas y matemáticas que poseen cada uno de los elementos del sistema que se desea representar. Es recomendable que el sistema comience con una representación simple y posteriormente se incremente el nivel de complejidad.

3. Colección de datos: la obtención de datos es un paso muy importante en la modelación debido a que indican las relaciones entre los elementos del sistema y muestran el comportamiento del mundo real.

4. Codificación del modelo: en esta fase se requiere de la programación del modelo matemático a instrucciones ejecutables por una computadora con el fin de que esta herramienta facilite las operaciones complejas que la simulación necesita.

5. Validación: posteriormente de la codificación es necesario validar que los resultados arrojados por el programa sean coherentes con los datos del sistema real. Esto es importante para comprobar que los datos son útiles y que podrán ser utilizados en el diseño de experimentos y en el análisis de resultados.

6. Experimentación: en esta fase es cuando se pueden plantear diversos escenarios que permiten la experimentación con los datos y el funcionamiento del sistema. Sin embargo es necesario haber validado dichos datos anteriormente.

7. Resultados: el análisis de los diferentes experimentos generará un conjunto de resultados que nos ayudarán a entender el funcionamiento del sistema real e incluso pronosticar comportamientos del sistema bajo determinadas circunstancias.

8. Implementación: finalmente el modelo se adaptará para se utilizado formalmente para su propósito durante su tiempo de vida (el tiempo en el que es válido el modelo).

Una herramienta común para calcular los valores de las variables de estado de los modelos de simulación discreta es la técnica Monte-Carlo. Esta es un método numérico utilizado para calcular sumas e integrales, útiles en las operaciones de dichas variables. A continuación se describe brevemente esta técnica.

2.1.3. Técnica Monte-Carlo

La técnica Monte-Carlo es un método numérico que estima parámetros estocásticos y deterministas basado en muestreos aleatorios. Esta técnica es utilizada para evaluar integrales múltiples, inversión de matrices, etc.(Taha, 2011) Actualmente existen diversas variantes del algoritmo; sin embargo, a continuación se resumen los pasos más importantes para su implementación.

1. Definir el posible dominio de las entradas.
2. Generar datos de entrada aleatoriamente con base en una distribución de probabilidad que se ajuste al dominio.
3. Desarrollar un calculo determinista sobre las entradas.
4. Agregar los resultados.

Por ejemplo, si se pretende estimar el valor de π con esta técnica; entonces, el primer paso consiste en definir el dominio de las entradas, es decir, en este ejemplo se dibuja un círculo dentro de un cuadrado unitario de manera que el cociente del área del círculo y la del cuadrado sea igual a $\pi/4$.

Posteriormente se colocan varios puntos aleatoriamente y de manera uniforme sobre el cuadrado (Paso 2). Luego, se calcula el número total de puntos y el número de puntos ubicados dentro del círculo (Paso 3).

Finalmente se estima el cociente del número de puntos dentro del círculo y el número total de puntos; entonces, π es igual a cuatro veces este valor (Paso 4). La Figura 2.2 muestra el resultado de la simulación anterior. En la gráfica se exhiben además el número total de puntos colocados simulados (n) y el valor aproximado de π.

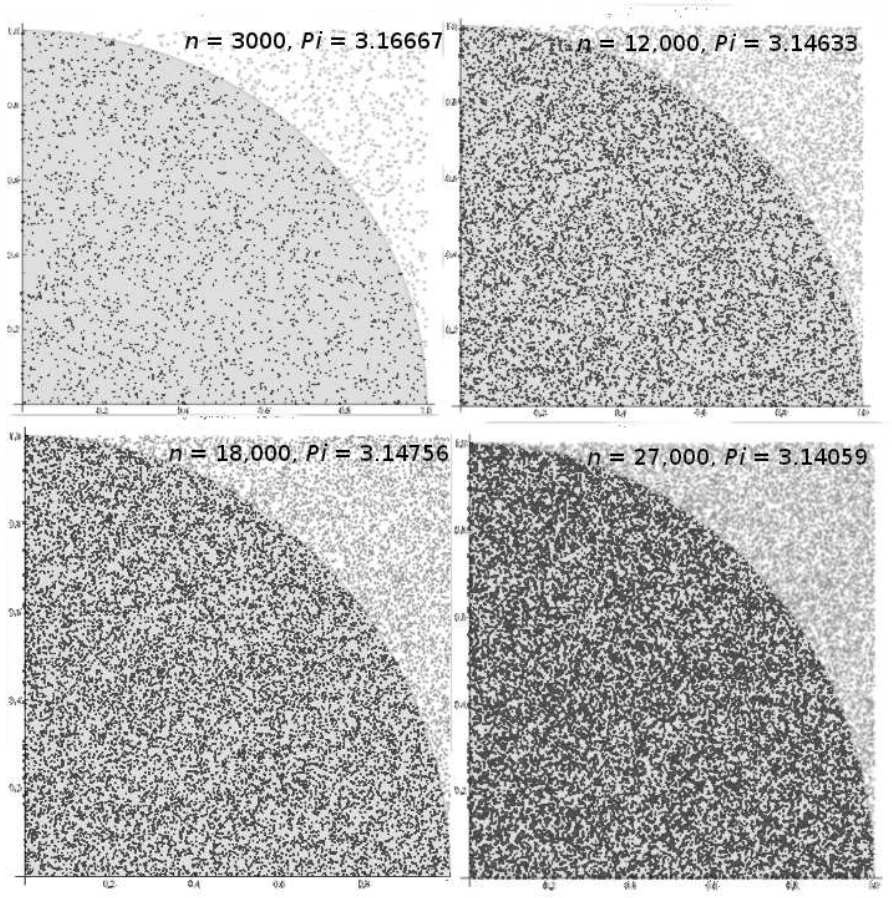


Figura 2.2: Resultados de la estimación de π con el método Monte-Carlo

Una herramienta común para validar o comparar el ajuste del modelo de simulación y los datos reales es a través de las pruebas de bondad de ajuste. Una de las pruebas de bondad de ajuste más utilizadas es la prueba χ^2, la cual es utilizada en variables tanto cualitativas y cuantitativas. A continuación se describe brevemente esta prueba.

2.1.4. Prueba de bondad de ajuste χ^2

La prueba de bondad de ajuste χ^2 o de Karl Pearson es una prueba estadística que se utiliza para saber si los resultados de la realización de varios en-

sayos multinominales se ajustan a un conjunto de datos de referencia. Estos datos multinominales son variables que estan conformadas por dos o más categorías; por ejemplo, el resultado del lanzamiento de un dado es una variable que está conformada por 6 categorías que corresponden a las frecuencias de ocurrencia de cada uno de sus lados.

El procedimiento general de la prueba consiste en:

- Distribuir los datos muestrales en k categorías mutuamente excluyentes.
- Obtener el estadístico χ^2 a través de la siguiente ecuación:

$$\chi^2 = \sum_{i=1}^{k} \frac{(o_i - e_i)^2}{e_i}$$

  donde: o_i es el valor observado en la categoría i; y e_i es el valor esperado en la categoría i

- Si hay un buen ajuste, las diferencias en la ecuación serán pequeñas, el numerador también y en concecuencia el valor del estadístico de la prueba. Si existen grandes discrepancias el valor del estadístico será grande.
- Si el valor calculado de χ^2, a partir de los datos estadísticos de la muestra, es mayor que el porcentil de la χ^2 (con los grados de libertad correspondientes), entonces se rechaza la hipótesis de que los datos tengan un ajuste similar.

2.2. Programación entera

En ocasiones es necesario utilizar modelos matemáticos que resuelvan un problema de la "mejor manera". Sin embargo, las técnicas de simulación no son adecuadas para este objetivo; por lo tanto, son necesarios modelos analíticos que tengan el objetivo de brindar una solución óptima; es decir, utilizar modelos de optimización.

Los modelos de optimización se dividen principalmente en modelos lineales y no-lineales. Sin embargo, a pesar de que las funciones lineales son funciones simples, son utilizadas frecuentemente en áreas económicas, en la planeación de la producción, en redes, en problemas de asignación, etc. De manera general, los modelos de programación entera son representados de la siguiente manera (Griva, 2009):

$$Max : z = \sum_{j=1}^{m} c_j x_j$$
$$\text{Sujeto a: } \sum_{j=1}^{m} a_{ij} x_j \leq b_i,$$
$$i = 1 \ldots n,$$
$$x_j \geq 0, x_j \in Z$$
$$j = 1 \ldots m$$

Donde una función objetivo lineal es optimizada con base en ecuaciones e inecuaciones que la restringen.

Existe un subconjunto de modelos de programación entera llamados modelos de programación entera binarios con diversas aplicaciones en el área de planeación. Los modelos de programación entera binarios, son modelos de programación entera dónde las variables de decisión sólo pueden tener los valores de 0 ó 1. Estos modelos tienen diversas aplicaciones, entre las que destaca la planeación. Lo anterior se debe a que las variables de decisión pueden representar un conjunto de actividades que pueden ser llevadas a cabo (si tienen un valor de 1) ó no (si tienen un valor igual a 0). Estos modelos se representan en forma matricial de la siguiente manera:

$$Min : z = c^T x$$
$$\text{Sujeto a: } Ax \geq b, x \in 0, 1$$

Para ejemplificar este tipo de modelos, a continuación se muestra un problema propuesto por Hamdy Taha (Taha, 2011):

"Cinco proyectos están siendo evaluados para un plazo de 3 años. La Tabla 2.1 brinda las ganancias esperadas de cada proyecto así como los gastos involucrados en cada año. ¿Qué proyecto debe ser seleccionado para maximizar las ganancias de acuerdo con el capital disponible en cada año? "

Cómo el objetivo es conocer los proyectos que maximizarían los beneficios, un modelo cuyas variables de decisión indiquen si el proyecto es implementado (1) o no (0) es adecuado.

$$x_j = \begin{cases} 0 & \text{Si el proyecto j no es elegido} \\ 1 & \text{Si el proyecto j es elegido} \end{cases}$$

Proyecto	Costos x año $M			Ganancias $M
	1	2	3	
1	5	1	8	20
2	4	7	10	40
3	3	9	2	20
4	7	4	1	15
5	8	6	10	30
Recursos $M	25	25	25	

Tabla 2.1: Tabla de datos de los proyectos a evaluar

Por otra parte, la función objetivo del modelo es maximizar los beneficios de la inversión, por lo tanto, se expresa de la siguiente manera:

$$Max : z = 20x_1 + 4Ox_2 + 20x_3 + 15x_4 + 30x_5$$
Sujeto a:
$$5x_1 + 4x_2 + 3x_3 + 7x_4 + 8x_5 \leq 25$$
$$x_1 + 7x_2 + 9x_3 + 4x_4 + 6x_5 \leq 25$$
$$8x_1 + 10x_2 + 3x_3 + x_4 + 10x_5 \leq 25$$
$$x_i \in \{0, 1\}$$

La solución óptima para el problema anterior es implementar todos los proyectos excepto x_5

2.3. Metodología de análisis y tratamiento de riesgos informáticos

La metodología de análisis y tratamiento de riesgos informáticos propuesta en el presente trabajo se divide en dos bloques principales: el primer bloque corresponde el análisis y la estimación de riesgos informáticos; y el segundo bloque, al tratamiento de riesgos a través de un modelo de programación entera binaria. Para el diseño de esta metodología se utilizó como base la metodología de construcción de modelos de simulación de Jerry Banks (Banks, 1998); además, se integró un proceso para la formulación de un modelo de optimización una vez que el análisis de riesgos se ha llevado a cabo. A continuación se describe los pasos principales de la metodología propuesta.

1. Análisis de riesgos informáticos
    a) Recolección de incidentes informáticos
    b) Análisis y procesamiento de incidentes informáticos
        1) Identificación de incidentes y escenarios
        2) Análisis de incidentes informáticos
        3) Identificación y análisis de impactos
        4) Niveles de criticidad y plan de actividades
    c) Formulación del modelo de simulación y ejecución de escenarios
    d) Interpretación de resultados
2. Plan de tratamiento de riesgos
    a) Desarrollo de la lista de actividades de mitigación de incidentes
    b) Identificación de restricciones de la lista de actividades de mitigación de incidentes
    c) Formulación y solución del modelo de programación entera.
    d) Interpretación de resultados

2.3.1. Recolección de incidentes informáticos

Los registros de incidentes informáticos son una fuente importante de información para el análisis de dichos sucesos dentro de una organización.

Una manera para obtener la información de incidentes informáticos dentro de una organización es el uso de un sistema de reporte de incidentes; este es un conjunto de procedimientos administrativos que permiten el registro de este tipo de sucesos. La Figura 2.3 muestra un ejemplo de la información necesaria en el reporte de incidentes; por ejemplo, el tipo de incidente, el impacto que provocó, la duración del mismo, etc.

Reporte de incidentes *Identificación del incidente*					
No. de incidente		Fecha y hora de notificación		Fecha y hora de ocurrencia	
Descripción del inicdente					
Detalles del incidente					
Activo afectado					
Propiedad afectada	Integridad [ ]		Confidencialidad [ ]		Disponibilidad [ ]
Impacto en la organización	Económica ($)		Productividad (Hrs.)		
Solución del incidente					
Medidas tomadas para contener el incidente					
Medidas tomadas para solucionar el incidente					
Persona encargada en supervisar el incidente					
Fecha y hora de la conlusión del incidente					

Figura 2.3: Ejemplo de formato para el reporte de incidentes informáticos. *Fuente: elaboración propia*

2.3.2. Análisis y procesamiento de incidentes informáticos

Después de la recolección de los incidentes informáticos, es necesario analizar dicha información con el fin de obtener dos datos importantes: la frecuencia de los diferentes tipos de sucesos, y el impacto que pueden tener dentro de la organización. Para lo cual, la presente metodología propone un conjunto de actividades de análisis y procesamiento que se detallan a continuación.

2.3.2.1. Identificación de incidentes y escenarios

El análisis de los incidentes informáticos comienza con clasificar a todos los incidentes que ocurrieron dentro de la organización. Algunos ejemplos de estas categorías pueden ser: incidentes producidos por ataques externos, incidentes ocurridos por falta de mantenimiento, incidentes provocados por errores humanos, etc. Cabe destacar que estos conjuntos son mutuamente excluyentes;

por lo tanto, si un incidente i_1 pertenece a la categoría I_1, entonces i_1 no debe pertenecer a las otras categorías.

Por otro lado, la metodología que se propone considera que la ocurrencia de los incidentes informáticos varia de acuerdo con una serie de actividades o «escenarios» que realiza una organización; por ejemplo: auditorías, periodos vacacionales, periodos de proyectos externos, eventos públicos, etc. Por esta razón es importante identificar los incidentes que ocurrieron durante estos escenarios.

2.3.2.2. Análisis de incidentes informáticos

Para llevar a cabo el análisis de los incidentes informáticos, se realiza una tabla donde se identifique la probabilidad de ocurrencia de cada tipo de incidente en cada uno de los escenarios previstos. Por ejemplo, la siguiente matriz representa los diferentes subconjuntos de incidentes ($I_{i,j}$) en una organización que identificó m categorías de incidentes, y n tipos de actividades.

$$I_{i,j} = \begin{pmatrix} I_{1,1} & I_{1,2} & \cdots & I_{1,n} \\ I_{2,1} & I_{2,2} & \cdots & I_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ I_{m,1} & I_{m,2} & \cdots & I_{m,n} \end{pmatrix}$$

En la matriz anterior, los elementos $I_{i,j}$ representan a conjuntos de incidentes de tipo i que ocurrieron durante el escenario j; por lo tanto, la probabilidad de que ocurra un incidente $I_{i,j}$ se calcula a través de la cantidad de elementos del conjunto $I_{i,j}$ dividido por la suma de incidentes de cada categoría establecida; es decir:

$$P(I_{i,j}) = \frac{|I_{i,j}|}{|I_{1,j}| + |I_{2,j}| + |I_{3,j}| + \cdots + |I_{m,j}|}$$

2.3.2.3. Identificación y análisis de impactos

Los impactos son daños que provocaron los incidentes dentro de la organización. Estos pueden ser de diversos tipos; sin embargo, los más comunes son los económicos, de productividad y de reputación. Por lo tanto, es importante identificar estas pérdidas para cada tipo de incidente.

Durante esta actividad, se identifica si los daños provocados por los incidentes siguen una tendencia que pueda ser modelada a través de una función de probabilidad; de lo contrario, establecer empíricamente los valores de probabilidad que se asemejen al caso estudiado. Este análisis análisis debe llevarse a cabo para cada categoría de incidentes.

Una manera para elegir la distribución de probabilidad del impacto de los riesgos puede ser la ubicación de los datos atípicos, si los datos son simétricos o asimétricos, o si los datos tienen un valor central (Damodaran, 2007). La figura 2.4 representa un diagrama de flujo para la elección de distribuciones de probabilidad. Por ejemplo, el impacto de algunos incidentes son asimétricos y presentan casos atípicos en valores altos, entonces una función exponencial representaría mejor estos datos.

Por otro lado, se deben realizar pruebas de ajuste para saber si la distribución elegida es adecuada. Actualmente se hacen distintos esfuerzos para estudiar el comportamiento de incidentes informáticos (Kuhl et al., 2008); en este sentido, algunos estudios relacionados con el ajuste de funciones en la detección de intrusos se han llevado a cabo (Park, 2005).

2.3.2.4. Niveles de criticidad y plan de actividades

El análisis de riesgos a través de incidentes que se propuso también considera dos parámetros importantes que deben establecer los tomadores de decisiones dentro de la organización. Por un lado, es necesario clasificar la criticidad de los impactos encontrados de acuerdo con los intereses de la organización; y por el otro lado, un plan de actividades acordes con los escenarios analizados previamente.

La criticidad de impactos es una serie de rangos de impactos que son de interés para la organización. Por ejemplo, se puede etiquetar como impactos «bajos» un rango de daños menores a una constante a, e impactos «moderados» al rango mayor a a, pero menor a una constante b; es decir, $a <$moderados$\leq b$. Esta información será útil para integrar los resultados del análisis de riesgos a un modelo de optimización.

Por otra parte, el plan de actividades son un conjunto de escenarios que la organización quiere pronosticar (ver sección 2.3.2.1); por ejemplo, si se establecieron los escenarios: e_1 =auditorías, e_2 =vacaciones, e_3 =proyectos externos y e_4 =evento públicos; un plan de actividades podría ser la lista: $\{e_1, e_3, e_3, e_1,$

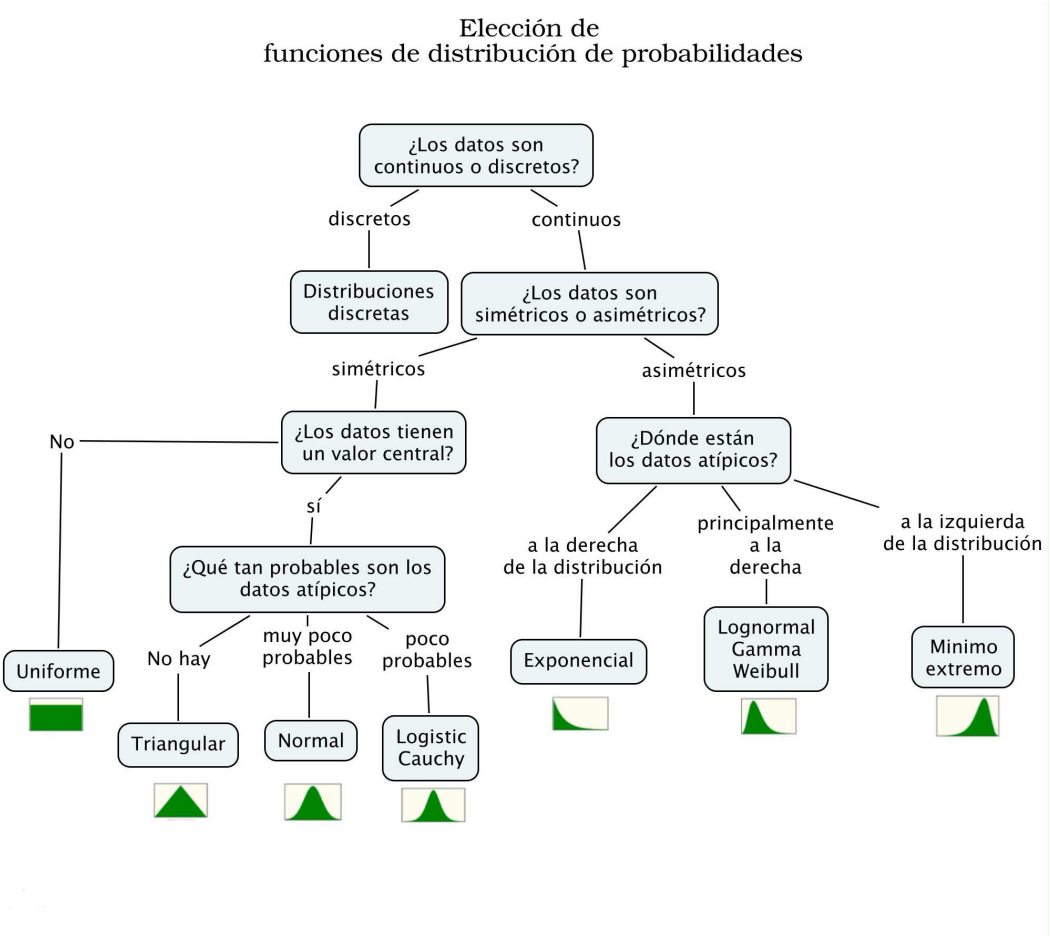


Figura 2.4: Diagrama de flujo para la elección de una distribución de probabilidad. *Fuente: elaboración propia basada en (Damodaran, 2007).*

e_2}. la cual representa un periodo de auditorías, seguido de dos periodos de proyectos externos, nuevamente un periodo de auditoría y finalmente un periodo vacacional. Este plan de actividades es la guía que utiliza el modelo para realizar pronósticos de incidentes durante la simulación.

2.3.3. Formulación y ejecución de la simulación

La información recabada de los incidentes informáticos es utilizada como variables aleatorias y parámetros constantes con el fin de construir el modelo de simulación. Estas variables toman diferentes valores de acuerdo con una función de probabilidad con el fin de generar datos artificiales que «se comportan similar al sistema real». La Figura 2.5 muestra las variables aleatorias que el modelo de simulación utilizó i.e. (1) El número de incidentes que se genera por cada tipo de incidente, y (2) El impacto de cada incidente. El diagrama también muestra la constante que se utilizó para definir la criticidad del incidente (3) y el escenario para experimentar (4).

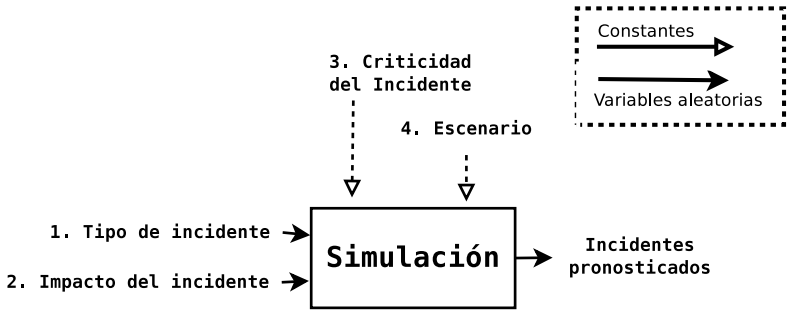


Figura 2.5: Diagrama de caja de las variables de estado. *Fuente: elaboración propia.*

Por otra parte, la técnica Monte-Carlo es un método numérico para determinar el valor de variables y parámetros ya sean aleatorias o deterministas. En este sentido, esta técnica fue utilizada para determinar incidentes informáticos de acuerdo con su probabilidad de ocurrencia, su impacto y las circunstancias que influyen para que estos sucedan (escenarios).

La Figura 2.6 muestra el proceso de simulación. El programa de simulación comienza por (1) extraer cada elemento e_i del plan de actividades E que establecieron los tomadores de decisiones; posteriormente dependiendo del

escenario e_i que se esté analizando (2) se genera un conjunto de incidentes i_n genéricos. La cantidad n de estos incidentes es un número aleatorio entre el mínimo y máximo de incidentes encontrados en el escenario e_i según los registros de incidentes anteriores. Después (3) se asigna una categoría I_i a cada i_n generado de acuerdo con la matriz mencionada en la sección 2.3.2.2. Una vez que se definen las categorías, es posible (4) asignar a cada incidente i_n un impacto. Este impacto dependerá de la función de probabilidad que corresponda a su categoría. Por lo tanto, la simulación arrojará una lista de incidentes con dos datos importantes: el tipo de incidente y su impacto.

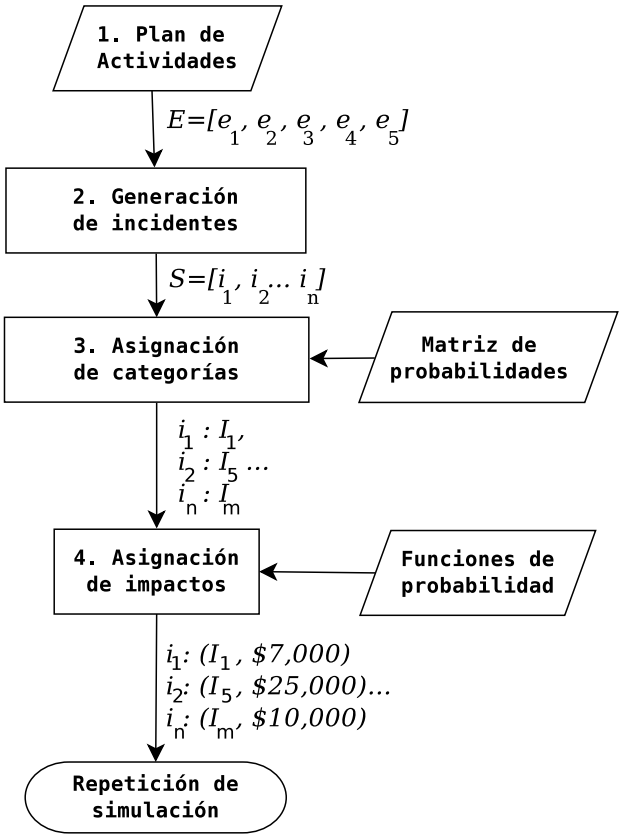


Figura 2.6: Diagrama del algoritmo de simulación utilizado. *Fuente: elaboración propia*

2.3.4. Resultados de la simulación

El modelo de simulación crea artificialmente diferentes tipos de incidentes informáticos así como sus impactos en cada prueba que se ejecuta; posteriormente, estos resultados se van promediando con respecto a cada ejecución de la simulación. A partir de estos resultados se puede obtener dos datos importantes: el total de incidentes estimados, y el total de impactos por tipo de incidente y categoría. Estas datos se resumen en la matriz de incidentes simulados S y la matriz de impactos R que se muestra a continuación.

$$S_{i,j} = \begin{pmatrix} S_{1,1} & S_{1,2} & \cdots & S_{1,n} \\ S_{2,1} & S_{2,2} & \cdots & S_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ S_{m,1} & S_{m,2} & \cdots & S_{m,n} \end{pmatrix}$$

Donde el elemento $S_{i,j}$ expresa **la cantidad de incidentes** de tipo i con un nivel de criticidad j.

Sin embargo, para obtener resultados más estables se ejecutan diversas pruebas de la simulación; por lo tanto, se deben promediar los diferentes resultados obtenidos en las diferentes pruebas generando una la matriz final S' que representa dicho promedio.

$$S' = \frac{1}{n} \sum_{i=1}^{n} S_n$$

donde n representa el total de las pruebas de simulación y S_n representa a la matriz $S_{i,j}$ en cada prueba n

Por otro lado, la matriz R representa **la suma de los impactos** para cada grupo de incidentes i de acuerdo con su nivel de criticidad j. Esta matriz se denota de la siguiente manera.

$$R_{i,j} = \begin{pmatrix} R_{1,1} & R_{1,2} & \cdots & R_{1,n} \\ R_{2,1} & R_{2,2} & \cdots & R_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ R_{m,1} & R_{m,2} & \cdots & R_{m,n} \end{pmatrix}$$

De la misma manera que la matriz anterior, los resultados de las diferentes pruebas n se promedian generando la matriz R' de la siguiente manera.

$$R' = \frac{1}{n} \sum_{i=1}^{n} R_n$$

donde n representa el total de las pruebas de simulación y R_n representa a la matriz $R_{i,j}$ en cada prueba n

Los resultados de la matriz R' son importantes para formular la función objetivo del modelo de optimización utilizado en las siguientes fases de la metodología.

2.3.5. Desarrollo de la lista de actividades de mitigación de incidentes

La segunda fase de la metodología propuesta tiene como objetivo mitigar cada grupo de riesgos informáticos ($R'_{i,j}$) encontrados en la fase de análisis. Estos grupos de riesgo se minimizan a través de grupos de controles de seguridad que la organización establece. Por lo tanto, los expertos de seguridad deben generar una grupo de contra-medidas para cada riesgo; y a cada grupo de contra-medida se le asignará una variable X_{ij}. Por ejemplo: el grupo de riesgos $R'_{1,1}$ se debe mitigar con el grupo de contra-medidas $X_{1,1}$, el grupo $R'_{1,2}$ con los controles $X_{1,2}$; y sucesivamente, el grupo $R'_{m,n}$ con los controles $X_{m,n}$.

Estos grupos de controles deben considerar a controles técnicos como antivirus, detectores de intrusos, filtros de tráfico, etc.; además de controles administrativos como: políticas de seguridad, y mejores prácticas.

2.3.6. Identificación de costos y restricciones de los grupos de contramedidas

El costo de los controles de seguridad, y el presupuesto de la organización son dos datos que deben tomarse en cuenta en la elaboración de un plan de tratamiento de riesgos. Un plan de tratamiento de riesgos no factible en costos que es llevado a cabo por una organización resulta en un plan de seguridad incompleto que pone en riesgo a la organización.

Para considerar estos datos en el modelo es importante identificar el costo total $C_{i,j}$ de cada grupo de controles $X_{i,j}$. Además, para hacer más robusto el modelo pueden considerarse diferentes tipos de costos como: financieros, horas invertidas, personal requerido, etc.

Por otro lado, deben considerarse los presupuestos que la organización destinará al plan de tratamientos de riesgos. Por tal motivo, la metodología utiliza un modelo de programación entera binaria que permite conocer la combinación de controles óptima de acuerdo con el presupuesto de la organización.

2.3.7. Formulación y solución del modelo de programación entera

El modelo de programación entera para el plan de tratamiento de riesgos consiste en un modelo matemático que permite elegir el grupo de controles de seguridad que deben implementarse para **minimizar el impacto de los grupos de riesgos** encontrados en la simulación. Este modelo considera las restricciones de presupuesto y el costo de los controles de seguridad. La Figura 2.7 ilustra la conexión entre el modelo de simulación y el modelo de programación entera. En el se puede observar que los resultados de la simulación son procesados para ingresarlos en la función objetivo del modelo de optimización. También se agregan a este modelo, datos relacionados con los recursos que tiene la organización y el costo de las actividades encaminadas a reducir el riesgo.

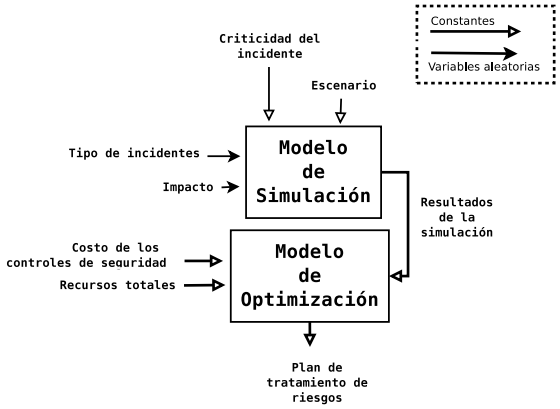


Figura 2.7: Conexión entre los modelos de simulación y optimización

$$Min : \sum_{j=1}^{m}\sum_{i=1}^{n} -R'_{ij}X_{ij}$$
$$\text{st. } \sum_{j=1}^{m}\sum_{i=1}^{n} C_{ij}X_{ij} \leq B$$
$$X_{ij} \in \{0,1\}, C \geq 0, B \geq 0$$
$$i,j \in N$$

El modelo de programación entera integra la matriz total de impactos R' en los coeficientes de la función objetivo, donde las variables de decisión son los grupos de controles de seguridad X_{ij}. Además, se consideran los costos C_{ij} de cada grupo de controles y el presupuesto B de la organización. La siguiente ecuación expresa lo mencionado anteriormente:

Por ejemplo, si el riesgo R_{11} corresponde al los impactos «bajos» de la categoría «ataques externos», entonces la actividad X_{11} representa a un conjunto de actividades tales como: realizar pruebas de vulnerabilidades, instalar equipos para la detección de intrusos, clasificar y proteger la información sensible, etc. Por lo anterior, la variable X_{11} se utiliza para decidir si este grupo es implementado o no. En el modelo las variables de decisión toman los siguientes valores binarios:

$$x_{ij} = \begin{cases} 1 & \text{Si la actividad se debe implementar} \\ 0 & \text{Si no} \end{cases}$$

2.3.8. Interpretación de resultados

El resultado final de los modelos es un vector de variables X_{ij} que representan a cada uno de los controles de seguridad que deben o no implementarse. Sin embargo, estos resultados deben considerarse como una herramienta para la toma de decisiones valiosa, que considera los aspectos principales de un problema complejo. Por lo tanto, los resultados deben tomarse en cuenta en la implementación de un plan de tratamiento de riesgos real, pero considerando que son resultados de un modelo abstracto y sintetizado.

Resumen

En esta sección se introdujeron brevemente los conceptos de simulación y programación entera: dos de las herramientas que se utilizaron en el desarrollo de

este trabajo. Posteriormente, se detalló la metodología que se propone en este trabajo en cada una de sus fases.

Capítulo 3

Análisis de riesgos informáticos: caso de estudio

En este capítulo se desarrolla la primera fase de la metodología de análisis y tratamiento aplicada a un caso de estudio; particularmente se detalla el proceso de la formulación del modelo de simulación de incidentes. La primera parte de esta capítulo trata sobre la obtención de los datos de entrada; posteriormente, la formulación de los parámetros de simulación (variables de estado); finalmente, la ejecución de la simulación y la discusión de los resultados de la misma.

3.1. Descripción del caso de estudio y recolección de datos

La UNAM ofrece diferentes tipos de servicios internos que son necesarios para las actividades académicas de la universidad. Por lo tanto, la información es uno de los activos más importantes que esta institución tiene.

Como se mencionó en el primer capítulo, la red UNAM es una de las infraestructuras tecnológicas más relevantes de esta institución, y cada año es un objetivo común de incidentes informáticos. Estos incidentes ocurren en las dependencias universitarias afectando sus activos. Por tal motivo se recopiló la información de estos sucesos en una de estas instituciones.

La dependencia, cuyo nombre no se menciona por razones de privacidad, tiene funciones en el área de tecnologías de información y comunicación de

la universidad. Esta institución reportó una serie de incidentes informáticos durante el periodo de 2011 y el primer semestre de 2012 que fue utilizada para llevar a cabo el estudio de análisis y tratamiento de riesgos presente en este trabajo.

La institución académica que se estudió cuenta con un sistema de reporte de incidentes informáticos que opera desde 2010. De esta base de datos se obtuvieron la información de 4 tipos de incidentes informáticos que ocurrieron durante el año 2011 y la mitad del 2012. Dicha información también reportó la cantidad de horas de productividad que la organización perdió en cada uno de los incidentes; por lo tanto, este dato fue considerado como el impacto o daño utilizado en los modelos propuestos.

3.2. Análisis y procesamiento de incidentes informáticos

La información de los incidentes informáticos fue analizada de acuerdo con la metodología descrita en el capítulo 2. A continuación se mencionan los incidentes que se analizaron para el presente estudio:

1. Incidentes por configuraciones inadecuadas de sistemas informáticos (C): estos incluyen todas las interrupciones a las actividades de la organización, la pérdida de datos o la incorrecta manipulación de información provocada por una configuración inadecuada de los sistemas informáticos. Por ejemplo, si se configura erróneamente un filtro de tráfico de red (firewall).

2. Incidentes provocados por intrusos (H): estos incidentes son aquellos que fueron provocados por usuarios mal intencionados que afectaron la información crítica de la organización; por ejemplo, un intruso modificando la página de internet de la organización.

3. Incidentes por falta de mantenimiento (M): estos fueron problemas en los sistemas informáticos ocurridos por la falta de mantenimiento de los equipos.

4. Incidentes provocados por violación de políticas (P): estos son percances provocados por la violación de las normas con las que se rige la organi-

zación, un ejemplo puede ser desechar información confidencial de una manera no adecuada a través del reciclaje de hojas.

Un total de 23 incidentes reportados durante 2011 (tabla 3.1) fueron analizados. Esta información arrojó que dichos eventos costaron aproximadamente **107 horas del tiempo de producción perdidas**.

Incidente	Mes	Tipo	Impacto (Hes.)
1	Enero	Cambios de configuración	10
2	Enero	Ataque externo	0.5
3	Enero	Cambios de configuración	1
4	Enero	Cambios de configuración	8
5	Enero	Cambios de configuración	24
6	Enero	Cambios de configuración	1
7	Febrero	Incumplimiento de política	1
8	Febrero	Incumplimiento de política	3
9	Marzo	Cambios de configuración	0.5
10	Marzo	Cambios de configuración	0.5
11	Marzo	Mantenimiento	0.6
12	Marzo	Cambios de configuración	0.6
13	Junio	Cambios de configuración	0.6
14	Julio	Mantenimiento	2
15	Agosto	Cambios de configuración	1
16	Agosto	Ataque externo	5
17	Agosto	Ataque externo	20
18	Agosto	Ataque externo	20
19	Octubre	Incumplimiento de política	3
20	Octubre	Incumplimiento de política	1
21	Octubre	Incumplimiento de política	3
22	Octubre	Cambios de configuración	0.5
23	Diciembre	Cambios de configuración	0.5
		Total	107.3

Tabla 3.1: tabla de incidentes ocurridos en 2011

También se recopiló información del primer semestre de 2012 (tabla 3.2). Sin embargo, esta información fue utilizada para la validación del modelo, por lo que no fue utilizada para la formulación del modelo de simulación.

Incidente	Mes	Tipo	Impacto (Hes.)
1	Enero	Incumplimiento política	8
2	Enero	Falta de mantenimiento	3
3	Enero	Ataque externo	0.5
4	Enero	Cambios de configuración	0.5
5	Febrero	Incumplimiento política	0.1
6	Febrero	Cambios de configuración	0.1
7	Febrero	Cambios de configuración	1
8	Marzo	Cambios de configuración	24
9	Marzo	Cambios de configuración	24
10	Marzo	Cambios de configuración	0.1
11	Marzo	Incumplimiento política	0.5
12	Abril	Ataque externo	0.5
13	Abril	Ataque externo	1
14	Abril	Cambios de configuración	0.1
15	Abril	Cambios de configuración	1
16	Mayo	Incumplimiento política	1
17	Mayo	Cambios de configuración	0.2
18	Junio	Falta de mantenimiento	3
19	Junio	Incumplimiento política	0.1
20	Junio	Cambios de configuración	0.25
21	Junio	Incumplimiento política	0.25
22	Junio	Cambios de configuración	0.5
23	Junio	Cambios de configuración	0.5
		Total	70.2

Tabla 3.2: tabla de incidentes ocurridos en 2012

3.2.1. Identificación de escenarios

Para conocer el funcionamiento real del sistema, se identificaron cuatro tipo de actividades que realizó la organización y que afectaron las probabilidades de ocurrencia de cada incidente informático. La tabla 3.3 muestra las actividades identificadas durante el año 2011.

La actividad marcada como «Auditoría» indica que la organización realizaba una auditoría durante este periodo de tiempo; generalmente durante estas actividades se reportan más incidentes debido a la supervisión constante de los auditores. La actividad «Proyecto Externo» señala una temporada en la que la organización trabaja con equipos de prueba o con terceros, por lo tanto, existen más probabilidades de que ocurran incidentes debido al cambio de configuraciones constante. Por otro lado, la actividad «Normal» indica una temporada donde no existe una actividad especial dentro de la organización y se caracteriza por una baja cantidad de incidentes. Finalmente la actividad «Evento Público» señala que la organización se involucró en actividades de carácter público y se caracteriza por una incidencia de ataques externos a la organización.

Mes	Actividad
Enero	Auditoría
Febrero	Proyecto Externo
Marzo	Proyecto Externo
Abril	Proyectos Externo
Mayo	Normal
Junio	Auditoría
Julio	Normal
Agosto	Evento Público
Septiembre	Normal
Octubre	Evento Público
Noviembre	Normal
Diciembre	Normal

Tabla 3.3: Actividades de la organización en 2011

3.2.2. Análisis de los incidentes informáticos

La fase de análisis informáticos, de acuerdo con la sección 2.3.2.2, requiere de la creación una tabla donde se expresen las probabilidades de ocurrencia de

los diferentes tipos de incidentes. La tabla 3.4 muestra las probabilidades de ocurrencia de cada incidente para cada actividad que la organización estableció. También se indica el número máximo y mínimo de incidentes que se debe simular.

Esta tabla se calculó a partir de la frecuencia de incidentes ocurridos durante 2011 (tabla 3.1) y la tabla de actividades correspondiente (tabla 3.3). Por ejemplo, los problemas de configuración durante las auditorías tienen una probabilidad de 0.86 (6/7). Este valor se obtuvo dividiendo el número de incidentes de configuración (C) durante los meses de auditoría (enero y junio) entre los siete incidentes que ocurrieron en este mismo periodo. Además, se tomó en cuenta el rango de incidentes por mes.

Incidente	P.Externo	Normal	Auditoría	E.Público
Hackers	0.00	0.00	0.14	0.375
Configuración	0.50	0.5	0.86	0.25
V.Política	0.33	0.00	0.00	0.375
Mantenimiento	0.17	0.50	0.00	0.00
Mínimos	2	0	1	4
Máximos	4	1	6	4

Tabla 3.4: Probabilidades y cantidades mínimas y máximas de cada tipo de incidente

3.2.3. Identificación y análisis de impactos

Otro dato importante para el cálculo del riesgo informático es el impacto que dañaría a la organización si ocurriera un percance. Este dato puede corresponder a pérdidas de tipo económicas, pérdidas de horas productivas, pérdidas de reputación, etc. En el caso de estudio, se consideraron las horas de productividad perdidas como la variable de impacto. Esta variable es aleatoria porque un mismo tipo de incidente puede afectar a la organización de diferentes maneras como se muestra en la columna «incidentes» de la tabla 3.1. Por lo tanto, fue necesario formular una función de probabilidad que imitara este comportamiento.

Estas funciones son importantes porque permiten obtener el impacto que posiblemente se tendría en la organización de acuerdo con el tipo de incidente que se esté simulando. Para obtener estas funciones se utilizó la tabla 3.1,

donde el impacto de los incidentes (C, H, M ó P) se ajustó con una función de distribución de probabilidad; los parámetros de estas funciones se obtuvieron a través de un software estadístico para obtener la curva correspondiente. A continuación se describe el proceso de análisis para cada tipo de incidente.

3.2.3.1. Incidentes por errores o cambios de configuración

Los incidentes producidos por errores o cambios en la configuración de los equipos informáticos son comunes cuando se implementan sistemas nuevos, o bien se les implementan nuevas funcionalidades. Es común que estos incidentes tengan un impacto bajo en una organización en ambientes controlados; es decir, los incidentes con un daño significativo son eventos atípicos en ambientes donde se monitorea el funcionamiento de los equipos informáticos.

El comportamiento del impacto que provocaron los incidentes ocasionados por errores y cambios de configuración se concentraron en rangos bajos como lo muestra la tabla 3.1; por lo tanto, se ajustó una función exponencial con parámetro $\lambda = 0.249$ que concentra las probabilidades en los impactos de nivel bajo y los incidentes con impacto alto son atípicos. En la figura 3.1 se muestra la función exponencial contrastada con el histograma de incidentes registrados.

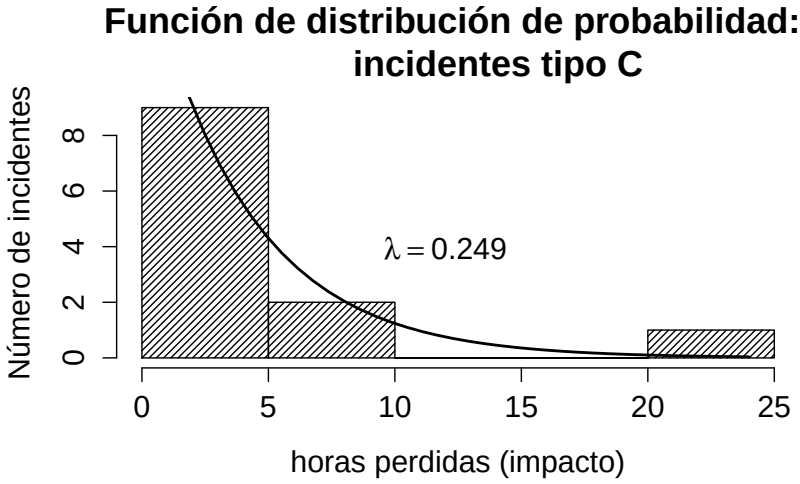


Figura 3.1: Distribución de probabilidad de los impactos de errores y cambios de configuración

Sin embargo, también se puede observar en la tabla 3.1 que tres de los doce incidentes de este tipo provocaron impactos de 8, 10 y 24 horas de productividad perdidas. Por lo que se decidió explorar un escenario adicional con la presencia de más casos atípicos de este tipo. Para elevar el número de casos atípicos se consideró la función beta mostrada en la figura 3.2 con parámetros $\alpha = 0.071$ y $\beta = 0.337$; la cual se comporta como una función exponencial en los primeros rangos de impacto, pero incrementa las probabilidades en el rango «atípico», provocando que la simulación genere este tipo de eventos.

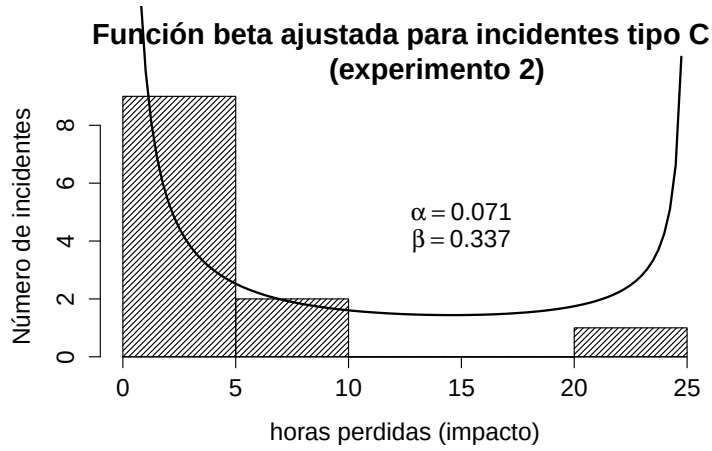


Figura 3.2: Distribución de probabilidad de los impactos de errores de configuración

Este experimento adicional es un ejemplo del potencial de la simulación que permite a los tomadores de decisiones calibrar el modelo y explorarlo situaciones de interés. Los resultados de este escenario reportaron que este tipo de incidentes tiene un mejor ajuste en los resultados de la simulación, mejorando sutilmente los resultados la prueba estadística χ^2 que se llevó a cabo en ambos modelos. Sin embargo, con el fin de no romper con la lectura de la revisión del primer escenario que se presenta en este capítulo, en el Anexo 1 de este trabajo se detalla el reporte de la simulación, y el plan de tratamiento de riesgos del segundo escenario.

3.2.3.2. Ataques externos

Los ataques externos son un tipo de incidente común en organizaciones con información accesible públicamente. Esto se debe a que puede ser objetivo de «escaneos aleatorios» que intrusos realizan en todo el mundo; además, si se trata de objetivos políticos, los ataques de hactivistas son una actividad común. Sin embargo, en la mayoría de las organizaciones, gran parte de los incidentes son mitigados por controles de seguridad utilizados frecuentemente en la infraestructura tecnológica; en otras palabras, los ataques exitosos que provocan un daño significativo suelen ser raros si se han implementado alguna medida de seguridad técnica; y en este sentido, una función de probabilidad exponencial generalmente modela este fenómeno, ya que esta distribución concentraría las probabilidades en los impactos bajos y disminuiría la probabilidad a medida que aparecerían los casos atípicos.

Sin embargo, en el caso de estudio se puede observar que los ataques externos provocaron la misma cantidad de impactos altos como bajos dentro de la organización. Considerando que los ataques con consecuencias graves fueron atípicos de acuerdo con los analísis de riesgos anteriores en los cuales no se encontraron casos de esta magnitud; estos registro se descartaron en el proceso de ajuste. El resultado que se obtuvo fue una función exponencial con parámetro $\lambda = 0.364$ que se muestra en la figura 3.3 donde se puede contrastar la función de probabilidad ajustada y el histograma de incidentes de este tipo; en la gráfica se puede observar que a medida que los impactos incrementan la probabilidad de ocurrencia disminuye de acuerdo con la curva de la función.

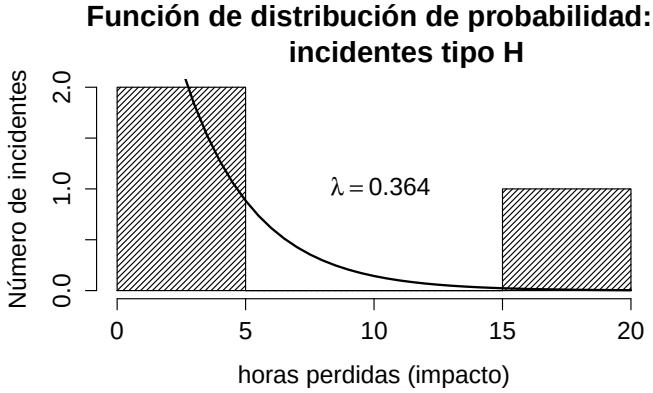


Figura 3.3: Distribución de probabilidad de ataques externos durante 2011

3.2.3.3. Incumplimiento de políticas de seguridad

Los incidentes provocados por la violación de políticas fueron ajustados con una distribución de probabilidad exponencial con un parámetro $\lambda = 0.455$. La figura 3.4 representa la función ajustada. En el eje x se muestran las horas perdidas de productividad y en el eje ordenado al origen el histograma de los incidentes. Debido a la escasa cantidad de datos que se recolectaron en el caso de estudio no se aprecia adecuadamente el ajuste de la función en contraste con el histograma de los datos recabados. De acuerdo con la teoría presentada en el segundo capítulo, se considera que estos incidentes siguen una tendencia exponencial cuando se revisa constantemente el cumplimiento de las políticas de seguridad ya que los incidentes más graves serían atípicos en escenarios controlados.

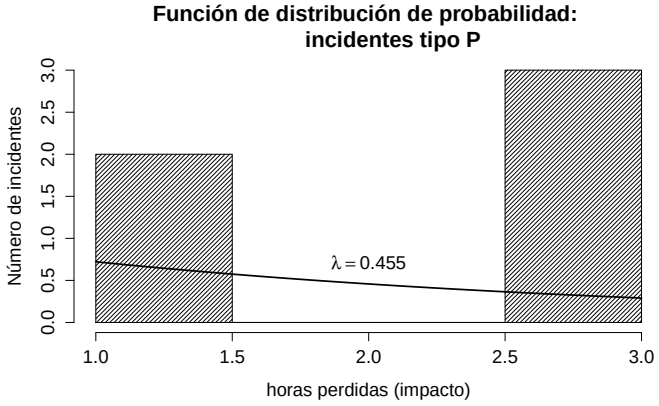


Figura 3.4: Distribución de probabilidad de las violaciones de políticas

3.2.3.4. Fallas por falta de mantenimiento

Los incidentes provocados por la falta de mantenimiento también fueron ajustados a través de una distribución exponencial con parámetro $\lambda = 2.5$. Los resultados del ajuste contrastados con el histograma se muestran en la figura 3.5 donde el eje de las x indica el impacto en hora, y el eje ordenado al origen muestra el histograma de los incidentes. Sin embargo, no muestran una tendencia en particular a causa de los pocos datos obtenidos.

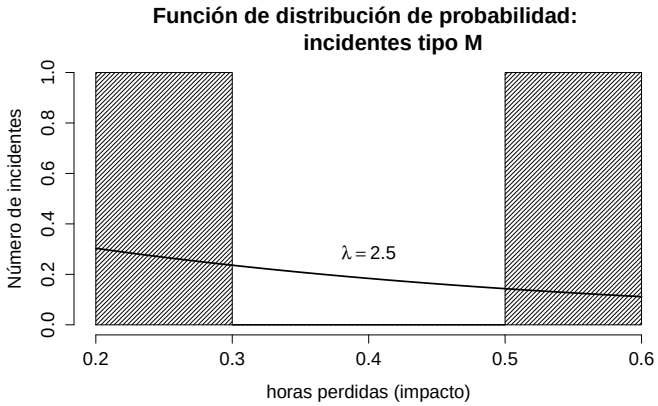


Figura 3.5: Distribución de probabilidad para incidentes por falta de mantenimiento

3.2.4. Niveles de criticidad y plan de actividades

La construcción del modelo de simulación requiere dos constantes como lo indica la metodología en la sección 2.3.2.4 La primera constante corresponde a un vector de rangos en el cual la organización define si el impacto de un incidente es alto, medio o bajo. El objetivo es clasificar el impacto para posteriormente formular un plan de tratamiento de riesgos.

La organización ha trabajado con tres rangos de impactos en otros análisis de riesgos. La tabla 3.5 indica los rangos que fueron establecidos para analizar el caso de estudio. El primero corresponde a impactos entre (0 a 5 horas), el segundo de (5.1 a 10 horas) y el último de (10.1 a 24 horas).

Impacto	Alto	Medio	Bajo
Rango	0-5	5.1-10	10.1-24

Tabla 3.5: Variable de criticidad

El otro dato importante para la elaboración del modelo de simulación es el plan de actividades a simular, el cual permite establecer las condiciones que serán analizadas durante las pruebas de simulación que se realicen. Para el caso de estudio analizado en este trabajo, el escenario corresponde al plan de actividades de la organización durante 2012 (tabla 3.6).

Plan de actividades 2012
Auditoría
Proyecto Externo
Proyecto Externo
Proyecto Externo
Auditoría

Tabla 3.6: Plan de actividades utilizado durante la simulación

3.3. Formulación y ejecución de la simulación

Las variables analizadas en la sección anterior fueron programadas en el lenguaje estadístico R(R Core Team, 2012). Este lenguaje permitió el manejo de las matrices y las tablas que manipularon los datos de dichas variables a través de un algoritmo basado en la sección 2.3.3.

La simulación comienza con la extracción de los elementos del plan de actividades contenidos en la tabla 3.6. Este plan permite calcular el número y tipo de incidentes que se generarán artificialmente de acuerdo con su probabilidad en la tabla 3.4. Una vez que se conoce el tipo de incidente, es posible calcular su impacto a través de la función de distribución de probabilidad que le corresponde (subsección 3.2.3).

El resultado de este proceso genera una lista de incidentes donde se especifica su tipo y su impacto en horas de productividad perdidas. La figura 3.6 muestra el resultado de ejecutar la función simulate_scenario. Esta función recibe dos variables: «a2012» que contiene el escenario y «prob» que contiene las tablas de probabilidades. Los resultados arrojados por esta simulación indican una lista de incidentes de tipo (C, H, M o P) y su impacto generado (columna impacts). En el ejemplo mostrado en esta figura se puede observar que se generaron 24 incidentes informáticos.

Finalmente, para determinar la matriz de resultados finales R' detallada en la sección 2.3.4, se efectuaron 100 simulaciones adicionales y se promediaron sus resultados. En la siguiente sección se describen y discuten dichos resultados.

```
> simulate_scenario(a2012,prob)
   f_incidents impacts
1            C    0.50
2            C    0.61
3            C    0.50
4            C   18.11
5            C    1.48
6            H    0.50
7            P    2.75
8            C    3.33
9            C    0.50
10           P    1.62
11           C    0.50
12           H    0.51
13           C   17.45
14           C    0.50
15           C    0.51
16           P    2.61
17           C    0.50
18           P    3.02
19           C    0.51
20           C    0.50
21           C   11.58
22           C    1.04
23           C    0.50
24           C    0.50
```

Figura 3.6: Ejecución de la simulación

3.4. Presentación y discusión de resultados de la simulación

La serie de simulaciones permitieron obtener la tabla de impactos R' que describe la suma de impactos de los doce grupos de incidentes resultantes. La tabla 3.7 muestra estos resultados.

	Total de impactos (Horas)			
Criticidad	C	H	M	P
Bajo	16.8	1.6	2.2	9.7
Medio	16.0	1.3	0	0
Alto	14.2	0.2	0	0
Total	47.0	3.1	2.2	9.7

Tabla 3.7: Tabla R: impacto de incidentes según su criticidad

La matriz de resultados S', donde se muestra el promedio de incidentes

generados en todas las simulaciones, combinada con la suma de impactos e la matriz R' permite calcular que en total se generaron 19 incidentes artificiales que provocaron 62.5 horas de productividad perdidas (tabla 3.8).

Tipo de incidente	Frecuencia	Impacto (Horas)
Errores de Configuración (C)	12	47.5
Ataques Externos (H)	1	3.1
Falta de Mantenimiento (M)	2	2.2
Incumplimiento de Políticas (P)	4	9.7
Total	19	62.5

Tabla 3.8: Resultados de la simulación

La figura 3.7 muestra la cantidad de cada tipo de incidente durante las 100 ejecuciones que se realizaron. Por otra parte, la figura 3.8 muestra el comportamiento de los impactos totales para cada tipo de incidente.

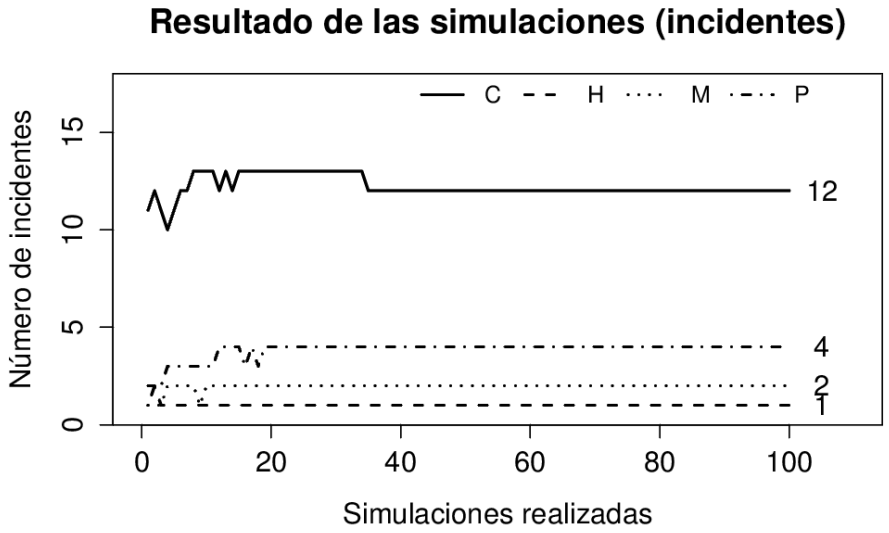


Figura 3.7: Comportamiento de la frecuencia de incidentes durante las simulaciones

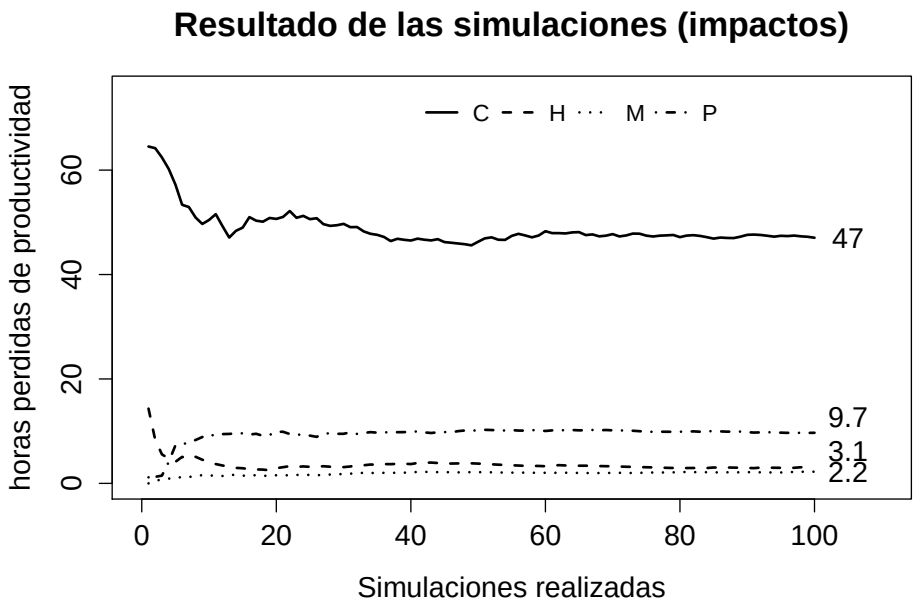


Figura 3.8: Comportamiento de los impactos de cada incidente durante las simulaciones

3.5. Validación de resultados

Los resultados de la simulación fueron validados con los reportes generados en 2012 a través de la comparación de gráficos, y analíticamente, a través de la prueba de bondad de ajuste χ^2 ya que este tipo de prueba es comunmente utilizado cuando los datos a validar están conformados por más de una categoría o grupo de datos; en este caso, el resultado de la simulación esta conformado por cada uno de los diferentes tipos de incidentes. Por otra parte, es importante recordar que los datos de 2012 no fueron utilizados para la formulación del modelo de entrada; en otras palabras, estos son independientes de la simulación.

La prueba de bondad de ajuste indicó que **no hay una diferencia estadística significativa entre el número de incidentes creados artificialmente por medio de la simulación y los datos obtenidos a través de los reportes**. A continuación se presentan estos resultados.

$$X_i^2 = \frac{(12-12)^2}{12} + \frac{(1-3)^2}{3} + \frac{(2-2)^2}{2} + \frac{(4-6)^2}{6} = 2$$

La prueba se calculó con 3 grados de libertad y un error de 5 %; como el valor de χ obtenido es menor al valor de la tabla ($2 < 7.81$), no existe una diferencia estadísticamente significativa entre el resultado y los datos reportados. Adicionalmente, la figura 3.9 muestra una comparación de la frecuencia de incidentes entre los resultados de la simulación y los que indicó el sistema de reportes de incidentes durante el primer semestre de 2012.

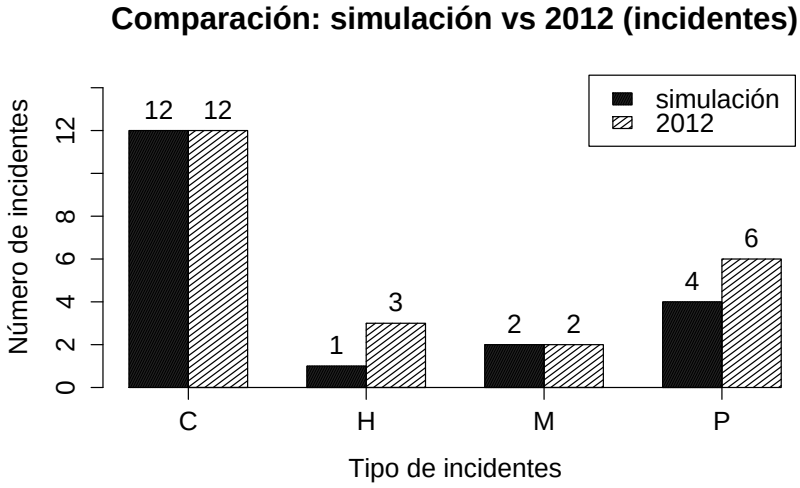


Figura 3.9: Validación de resultados (frecuencia de incidentes)

Por otro lado, la misma prueba aplicada a las horas perdidas de productividad muestra que **no existe una diferencia significativa entre la simulación y los datos observados; es decir, el modelo produce datos similares a los reales**. A continuación los resultados descritos.

$$X_i^2 = \frac{(47-52.2)^2}{52.2} + \frac{(3.1-2)^2}{2} + \frac{(2.2-6)^2}{6} + \frac{(9.7-9.9)^2}{9.9} = 3.53$$

Como se puede observar en los resultados, el valor de χ^2 fue menor al de la tabla calculado con tres grados de libertad y considerando un error del 5 %. La figura 3.10 muestra la comparación gráfica del impacto de los incidentes simulados y los reportados durante el primer semestre de 2012.

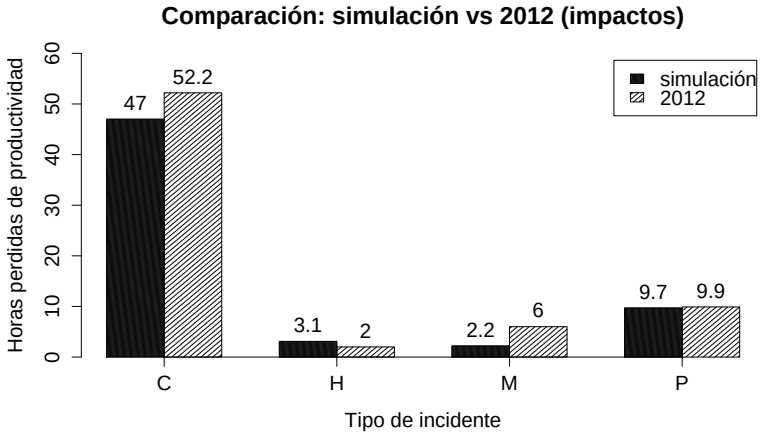


Figura 3.10: Validación de resultados (impacto de incidentes)

Resumen

En esta sección se revisó el modelo de simulación utilizado en la metodología de análisis de riesgos que se propone en este trabajo. Para ello se indicó la fuente de datos utilizada para llevar a cabo el estudio y se describió el modelo de simulación, donde se definieron las variables utilizadas para ejecutar la simulación del modelo. Además, se detalló la técnica utilizada en la simulación y se discutieron los resultados obtenidos. Sin embargo, estos resultados corresponden a la primera parte de la metodología; en la siguiente sección se describe el modelo de optimización utilizado en la segunda parte de la metodología: el tratamiento del riesgo.

Capítulo 4

Plan de tratamiento de riesgos: caso de estudio

En este capítulo se describe la segunda parte de la metodología para el análisis y tratamiento de riesgos informáticos. Específicamente se aborda el tema del modelo de programación entera binaria utilizado para formular un plan para mitigar los riesgos encontrados durante la simulación. La primera parte menciona la construcción del modelo a través de los resultados de la simulación; posteriormente, se menciona la solución del modelo y la discusión de los resultados.

De acuerdo con la información presentada en los primeros capítulos, los incidentes informáticos producen daños en la productividad, problemas financieros, de credibilidad, entre otros. Sin embargo, es posible reducir el impacto o la ocurrencia de dichos percances a través de mecanismos de seguridad o contra-medidas. Estos mecanismos de seguridad son medidas tecnológicas y administrativas que tienen como objetivo reducir el riesgo. Sin embargo, cada control de seguridad tiene un costo económico, además de consumir otros recursos como el personal que lo opera y el tiempo en que se implementan.

Para elegir adecuadamente los controles de seguridad informáticos necesarios para reducir el riesgo, algunos marcos de trabajo como el ISO 27001:2005 plantean realizar un análisis de riesgos que permite priorizar los incidentes de alto impacto y enfocar los recursos para mitigarlos. Una vez que se cuenta con esta información, es necesario relacionar cada potencial incidente con un conjunto de actividades que tienen el objetivo de impedir que ocurra este.

Un ejemplo de lo anterior es el código de buenas prácticas o controles de seguridad que sugiere el estándar internacional ISO/IEC 27002 (ISO/IEC, 2005b) en el que se describen un conjunto de actividades encaminadas a reducir el riesgo. El objetivo es que la organización prevenga los incidentes informáticos a través de un plan de actividades conocido como plan de tratamiento del riesgo.

4.1. Plan de tratamiento de riesgos

Debido a que el análisis de riesgos no sólo brinda información acerca del comportamiento de los riesgos, sino que también puede ser utilizado para reducir los incidentes de manera óptima a través del plan del tratamiento de riesgos, en este trabajo se propuso un modelo de optimización lineal, basado en los resultados del análisis de riesgos, para ayudar en la toma de decisiones en la reducción de los incidentes informáticos.

Como se mencionó en el segundo capítulo, los modelos de programación lineal, particularmente los modelos de programación entera binaria, permiten obtener la combinación óptima de soluciones para problemas de asignación. En el caso particular de los incidentes informáticos, se refiere a programar qué actividades o contra-medidas deben implementarse para reducir la mayoría de los inconvenientes provocados por los problemas informáticos.

4.1.1. Formulación del modelo de minimización del riesgo

El modelo de programación entera binario tiene como objetivo generar un plan de tratamiento de riesgos óptimo que consiste en encontrar un conjunto de actividades que minimicen el riesgo total de acuerdo con el presupuesto y tiempo con el que cuenta la organización. Para tal efecto, se plantearon las siguientes variables.

4.1.1.1. Variables de decisión

Debido a que el objetivo es encontrar un conjunto de actividades que minimicen el riesgo, se planteó un vector x_i que representa una actividad que le corresponde a una serie de buenas prácticas y contra-medidas que tienen como

objetivo mitigar el riesgo i. Por ejemplo, si el riesgo i es un incidente de ataque externo, entonces la actividad i representa a un conjunto de actividades tales como: realizar pruebas de vulnerabilidades, instalar equipos para la detección de intrusos, clasificar y proteger la información sensible, etc. Por lo anterior, la variable x_i debe ser establecida por un experto en seguridad de la información, y para decidir si es implementada o no, en el modelo toma los siguientes valores binarios:

$$x_i = \begin{cases} 1 & \text{Si la actividad se debe implementar} \\ 0 & \text{Si no} \end{cases}$$

4.1.1.2. Función objetivo

Una vez que las variables de decisión fueron establecidas, se formuló la función objetivo a optimizar de acuerdo con el modelo propuesto en la sección 2.3.7. Como se mencionó en el capítulo dos, el interés principal es minimizar el impacto de los riesgos informáticos identificados. Por lo tanto, se utilizó la tabla 3.7 del capítulo anterior, para definir los valores de la función objetivo. En esta tabla se concentran los diferentes impactos de los incidentes de acuerdo con su nivel de criticidad correspondiente. En este sentido, se asignó a cada grupo de riesgos una actividad x_i definida por las variables de decisión; entonces, la activación de la variable permite restar el impacto que le corresponde como la establece la siguiente la siguiente función:

$$min : -16.8x_1 - 16x_2 - 14.2x_3 - 1.6x_4 - 1.3x_5 - 0.2x_6 - 2.2x_7 - 9.7x_{10}$$

4.1.1.3. Restricciones

Finalmente, se establecieron las restricciones del problema. Estas restricciones corresponden a los recursos con los que cuenta la organización para implementar su plan de tratamiento de riesgos. El modelo debe tomar en cuenta estas restricciones ya que un plan de tratamiento ambicioso resultaría en una implementación no factible o fallida.

Para el caso de estudio se formularon una serie de restricciones basadas en el límite de tiempo que cuenta la organización para implementar un plan de tratamiento de riesgos (32 días) y el costo hipotético de la implementación de cada actividad que no debe rebasar $150,000. Estos valores se definieron de acuerdo con los valores establecidos en análisis de riesgos anteriores. La tabla

4.1 indica el número de días y el costo que se utilizaría para implementar la actividad x_i.

Restricción	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	x_9	x_{10}	x_{11}	x_{12}
Tiempo de implementación (días)	1	5	10	1	5	15	2	5	10	1	5	10
Costo ($×1000)	1	3	10	5	10	50	10	50	100	10	20	50

Tabla 4.1: Tabla de restricciones para el modelo de optimización

Cabe mencionar que aunque el tiempo para implementar una actividad sobrepasa el tiempo perdido por el incidente correspondiente, esto no significa que la organización pierde más tiempo en el control de seguridad que en el impacto del incidente ya que el impacto de cada riesgo corresponde a horas perdidas de productividad en toda la organización, y por el contrario, el tiempo de implementación sólo representan el tiempo invertido por el equipo de seguridad.

4.1.2. Modelo de optimización para el plan de tratamiento de riesgos

Una vez que se formularon la función objetivo y las restricciones, el modelo se definió de la siguiente manera:

$min : -16.8x_1 - 16x_2 - 14.2x_3 - 1.6x_4 - 1.3x_5 - 0.2x_6 - 2.2x_7 - 9.7x_{10}$
s.a.
$x_1 + 5x_2 + 10x_3 + x_4 + 5x_5 + 15x_6 + 2x_7 + 5x_8 + 10x_9 + x_{10} + 5x_{11} + 10x_{12} \leq 32$
$x_1 + 3x_2 + 10x_3 + 5x_4 + 10x_5 + 50x_6 + 10x_7 + 50x_8 + 100x_9 + 10x_{10} + 20x_{11} + 50x_{12} \leq 150$

4.2. Discusión de los resultados

El modelo fue resuelto a través del programa «lp_solve» (lp_solve Project Team, 2013), el cual es un software de código abierto que permite resolver programas enteros lineales mixtos (MILP por sus siglas en inglés). Este software fue elegido

porque puede utilizarse directamente sobre el código R con el que se realizó la simulación. Esto permite que no sea necesario trasladar los resultados de un software a otro; sino que la solución del modelo de optimización se realice dentro de la simulación.

A continuación se presenta el código, en lenguaje R, que permitió la solución del modelo. En el código se puede observar a la variable «PTR» que representa al modelo entero binario. También se puede observar a la función objetivo creada con la función «set.objfn» a la que se le agregaron los valores de cada coeficiente. Después se agregaron dos restricciones a través de la función «add.constraint». Adicionalmente, se se configuró el modelo PTR como tipo binario con la función «set.type»; finalmente, se obtuvo el valor de cada variable de decisión con la función «solve».

```
PTR<-make.lp(0,12)
set.objfn(PTR,c(-16.8,-16,-14.2,
                -1.6,-1.3,-0.2,
                -2.2,0,0,
                -9.7,0,0))
add.constraint(PTR,c(1,5,10,
                     1,5,15,
                     2,5,10,
                     1,5,10),
               "<=",32)
add.constraint(PTR,c(1,3,10,
                     5,10,50,
                     10,50,100,
                     10,20,50),
               "<=",150)

set.type(PTR,columns=c(1:12),type="binary")
solve(PTR)
```

Como resultado, el plan de tratamiento de riesgos consiste en la implementación de todas las actividades excepto la actividad 6 que corresponde al grupo de controles que mitigan los ataques externos graves. Este plan permite mitigar 61.8 de las 62.5 horas de productividad perdidas por los riesgos informáticos; cabe destacar que se consideraron los costos de cada actividad y el presupuesto de la organización. La Tabla 4.2 resume dichos resultados.

	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	x_9	x_{10}	x_{11}	x_{12}
Resultado:	1	1	1	1	1	0	1	0	0	1	0	0

Tabla 4.2: Resultados del modelo de optimización; Las variables con valor = 1 indican que la actividad debe implementarse, de lo contrario, la variable es igual a O.

Es importante concluir que estos datos deben ser utilizados como guía para la toma de decisiones y no como resultados definitivos debido a los diferentes supuestos que se utilizaron.

Resumen

En este capítulo se pudo observar la aplicación de los resultados de la simulación de incidentes informáticos para realizar un plan de tratamiento de riesgos. Un aspecto importante para esta tarea fue la integración de los resultados del modelo anterior a la función objetivo del modelo de optimización; además, la definición de restricciones y recursos con los que cuenta la organización. Los resultados fueron consistentes y coherentes; sin embargo, sólo deben ser utilizados como apoyo para la toma de decisiones debido a la naturaleza estocástica del problema. A continuación se presentan las conclusiones generales del trabajo de investigación.

Conclusiones

Durante el desarrollo de esta tesis se resaltó la importancia de la seguridad informática, la cual ha presentado un mayor auge a medida que las organizaciones y las personas utilizan con más frecuencia las tecnologías de información y comunicación.

Primero se analizaron algunas de las características que presenta esta problemática; en particular, el estudio se enfocó en los incidentes informáticos. Posteriormente se analizó una de las estrategias que se utiliza para afrontar estos sucesos: el análisis de riesgos.

Después, se discutieron las dos herramientas que se propusieron para el análisis y la solución analítica de problemas: la simulación y la programación entera. Lo anterior con el objetivo de presentar una metodología que combinó ambas herramientas para realizar un análisis de riesgos eficientemente. De esta manera, se aplicó la metodología de análisis y tratamiento de riesgos informáticos en un caso de estudio con los datos registrados en una institución de tecnologías de la información dependiente de la UNAM.

En este sentido, se cumplieron los objetivos que se plantearon al principio de este trabajo de investigación:

- La revisión bibliográfica permitió concluir que actualmente existen dos tipos de metodologías de análisis de riesgos: cualitativas y cuantitativas. Las primeras son útiles cuando no existen datos históricos que se pueda analizar; las segundas son más precisas en la estimación del riesgo cuando cuentan con los registros históricos suficientes.

- La revisión de las metodologías de análisis de riesgo permitió ubicar a la simulación como una herramienta versátil que permite estimar el riesgo adecuadamente, y facilita la exploración escenarios extremos o de interés.

También se destacó la programación entera como otra técnica útil para la planeación de estrategias de seguridad.

- La revisión del marco conceptual de las técnicas de simulación y programación entera permitieron construir una metodología de análisis y tratamiento de riesgos informático que combinó ambas herramientas.

- El análisis de datos los registros de incidentes informáticos del caso de estudio permitió la caracterización de cuatro tipos de incidentes informáticos de manera probabilística a través de las funciones exponencial y beta. Se encontró que la función exponencial es adecuada en situaciones donde los impáctos altos son atípicos; y por otra parte, la función beta es más adecuada cuando se desea plantear escenarios con impactos altos elevados dentro de la simulación. Ambas funciones fueron adecuadas para la modelación de este tipo de incidentes de acuerdo con la prueba estadística Chi^2.

- Finalmente, se logró presentar un plan de tratamiento de riesgos óptimo de acuerdo a los recursos de la organización estudiada.

Es importante resaltar que la metodología mostró su potencial para resolver el problema planteado en el estudio. Además, se logró una adecuada toma de decisiones en el tratamiento del riesgo informático, ya que los resultados en el caso de estudio fueron consistentes y significativos; por lo tanto, la metodología puede ser tomada como base para realizar futuros trabajos de investigación como: planes de continuidad del Negocio (BCP, por sus siglas en inglés) y planes de recuperación de desastres (DRP, por sus siglas en inglés).

Referencias

Aranda, J. (17-1-2013). Queda fuera la página web de sedena al ser hackeada. Periódico La Jornada en línea. `http://www.jornada.unam.mx/2013/01/17/`.

Banks, J. (1998). *Handbook of Simulation: Principles, Methodology, Advances, Applications, and Practice*. Wiley and Sons.

Buchanan, W. (2011). *Introduction to Security and Network Forensics*. CRC Press, 1 edition.

Caulkins, J. P., Hough, E. D., Mead, N. R., and Osman, H. (2007). Optimizing Invest-ments in Security Countermeasures: A Practical Tool for Fixed Budgets. *IEEE Security and Privacy*, pages 57–60.

Damodaran, A. (2007). *Strategic Risk Taking: A Framework for Risk Management*. Prentice Hall, 1 edition.

Garvey, P. R. (2009). *Analytical Methods for Risk Management*. Chapman and Hall CRC Press, 1 edition.

Gollman, D. (2011). *Computer Security*. Wiley and sons, 3 edition.

Griva, I. (2009). *Linear and Nonlinear Optimization*. SIAM, 2nd edition.

ISO/IEC (2005a). ISO/IEC 27001:2005 Information technology - Security techniques - Information security management systems - Requirements. Estándar internacional, International Organization for Stendarization, Geneva, Switzerland.

ISO/IEC (2005b). ISO/IEC 27002:2005 Information technology - Security techniques - Code of practice for information security management. Estándar

internacional, International Organization for Stendarization, Geneva, Switzerland.

ISO/IEC (2009). ISO/IEC 27000:2009 Information technology - Security techniques - Information security management systems - Overview and vocabulary. Estándar internacional, International Organization for Stendarization, Geneva, Switzerland.

Kuhl, M. E., Lada, E. K., Steiger, N. M., Wagner, M. A., and Wilson, J. R. (2008). Introduction to modeling and genereting probabilistic input processes for simulation. *Proceedings of the 2008 Winter Simulation Conference*, pages 41–61.

lp_solve Project Team (1-1-2013). lp_solve. En línea. `http://ipsolve.sourceforge.net`.

Park, Y. (2005). A statistical process control approach for network intrusion detection. *School of Industrial and Systems Engineering*, pages 1–99.

Pfleeger, C. P. and Pfleeger, S. L. (2003). *Security in Computing*. Prentice Hall, 4 edition.

PWC (1-11-2012). Information Security Branches. En línea. `http://www.pwc.co.uk/en_UK/uk/assets/pdf/olpapp/uk-information-security-breaches-survey-technical-report.pdf`.

R Core Team (1-7-2012). R: A language and environment for statistical computing. En línea. `www.r-project.org`.

Sahinoglu, M. (2005). Security Meter: A Practical Decision-Tree Model to Quantify Risk. *IEEE Security and Privacy*, pages 18–24.

Software Engineering Institute (1-11-2012). OCTAVE Allegro. En línea. `http://www.cert.org/octave/allegro.html`.

Taha, H. A. (2011). *Operations Research: An Introduction*. Prentice Hall, 9 edition.

UNAM-CERT (1-11-2012). Estadísticas. En línea. `http://www.cert.org.mx/estadisticas.dsc`.

Winkelvos, T., Rudolph, C., and Repp, C. (2011). A property based security risk analysis through weighted simulation. *Information Security South Africa (ISSA)*, pages 15–17.

Índice de figuras

Índice de tablas

Anexo I

El modelo de simulación, que se programó para llevar a cabo el análisis de riesgos de la metodología que se describe en este trabajo, permite explorar diversos escenarios de interés a los tomadores de decisiones; por tal motivo, se documentó un segundo experimento realizando algunas modificaciones al caso de estudio presentado en el capítulo 3 y 4.

4.3. objetivo

El objetivo de realizar este segundo experimento fue modificar los parámetros del modelo de la simulación para incrementar los casos de los incidentes de tipo C de alto impacto durante la simulación; adicionalmente, se buscó modificar el modelo de programación entera para forzar la implementación del grupo de controles de seguridad que mitiga los ataques externos graves, suponiendo hipotéticamente por motivos de normatividad.

4.4. Simulación

Los datos introducidos en este modelo fueron los mismos utilizados en los capítulos 3 y 4; sin embargo, se modificó la función de impactos para los incidentes de tipo C. En particular, se utilizó una función beta para forzar que el modelo de simulación generara impactos altos en los incidentes de esta categoría y así evaluar casos extremos. Esta función con parámetros $\alpha = 0.071$ y $\beta = 0.337$ (figura 4.1) se comporta como una función similar a la función exponencial en los primeros rangos de impacto, pero incrementa las probabilidades en el rango «atípico», provocando que la simulación genere este tipo de eventos.

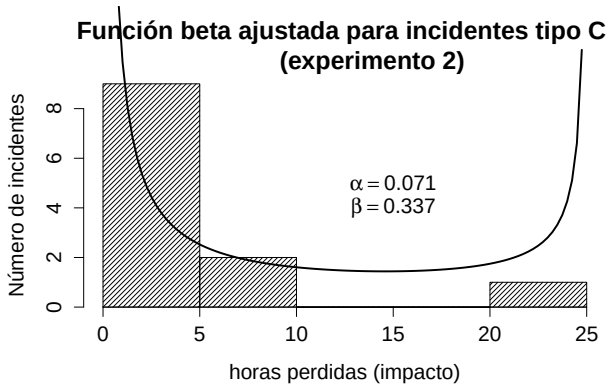


Figura 4.1: Distribución de probabilidad de los impactos de errores de configuración con función beta

4.5. Resultados del segundo experimento

Los resultados fueron consistente con lo esperado pues se incrementó el impacto producido por los incidentes de tipo C como se muestra en la figura 4.2, donde se presenta una comparación entre los impactos obtenidos por los dos experimentos y los reportes de 2012. Este incremento ocurrió porque la función beta crea más incidentes con nivel de impacto alto en la simulación.

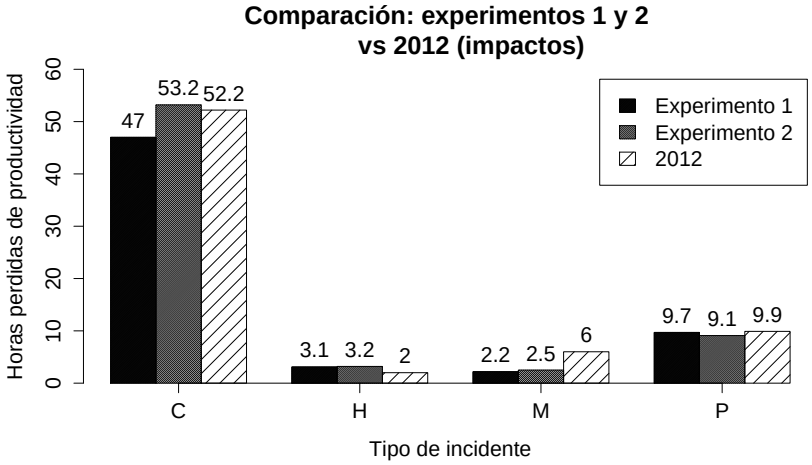


Figura 4.2: Comparación de resultados de los dos experimentos y los resultados reportados en 2012

Por otra parte, la prueba χ^2 aplicada a los resultados del segundo experimento mostró un mejor ajuste, ya que el valor obtenido (2.84) fue ligeramente menor al valor obtenido en el capítulo 3 (3.53).

4.6. Resultados del plan de tratamiento de riesgos en el segundo experimento

Los resultados en el plan de tratamiento de riesgos no se modificaron con el incremento del impacto en el segundo experimento. Sin embargo, con el objetivo de revisar dicho experimento en situaciones de interés, se modificó el modelo de optimización para forzarlo a elegir los controles que mitigan los ataques externos graves, suponiendo que los analistas del riesgo deben mitigar este tipo de riesgos problemáticos por motivo del cumplimiento de una normatividad. Esta modificación se realizó agregando la restricción $x_5 = 1$ provocando que los resultados del plan de tratamiento de riesgos cambiaran. Los resultados indicaron que se deben implementar las actividades: x_1, x_2, x_3, x_6 y x_{10} dejando fuera los controles que mitigan los incidentes por falta de mantenimiento.

4.7. Conclusiones del segundo experimento

El modelo permitió estudiar evaluar otros escenarios con la modificación de parámetros de la simulación, incluso estos nuevos escenarios pueden servir para obtener un comportamiento de interés a los tomadores de decisión, en este caso, incrementar el número de incidentes atípicos artificialmente. También el modelo de optimización permite realizar cambios en las restricciones permitiendo dar más opciones y alternativas a los tomadores de decisión.