INSTITUTO TECNOLÓGICO DE ESTUDIOS SUPERIORES DE MONTERREY

DIVISIÓN DE ELECTRÓNICA, COMPUTACIÓN, INFORMACIÓN Y COMUNICACIONES

PROGRAMAS DE GRADUADOS EN ELECTRÓNICA, COMPUTACIÓN, INFORMACIÓN Y COMUNICACIONES

Los miembros del comité de tesis recomendamos que la presente tesis del Ing. Carlos Alejandro Quintal Chay sea aceptada como requisito parcial para obtener el grado académico de Maestro en Administración de Telecomunicaciones.

Comité de tesis:

Dr. Jorge Carlos Mex Perera
Asesor

Dr. Juan Arturo Nolazco Flores
Sinodal

Ing. Alejandro Parra Briones
Sinodal

Dr. David Garza Salazar
Director del Programa de Graduados en Electrónica, Computación, Información y Comunicaciones.
Diciembre 2005

INSTITUTO TECNOLÓGICO Y DE ESTUDIOS SUPERIORES DE MONTERREY

CAMPUS MONTERREY

PROGRAMA DE GRADUADOS EN ELECTRÓNICA, COMPUTACIÓN, INFORMACIÓN Y COMUNICACIONES

"MODELOS DE SEGURIDAD DE LA INFORMACIÓN BASADOS EN SISTEMAS DINÁMICOS"

TESIS

PRESENTADA COMO REQUISITO PARCIAL PARA OBTENER EL GRADO ACADEMICO DE:

MAESTRO EN ADMINISTRACIÓN DE LAS TELECOMUNICACIONES

POR:
CARLOS ALEJANDRO QUINTAL CHAY

MONTERREY, N.L. DICIEMBRE 2005

“MODELOS DE SEGURIDAD DE LA INFORMACIÓN BASADOS EN SISTEMAS DINÁMICOS”

POR:
Carlos Alejandro Quintal Chay

TESIS

Presentada al Programa de Graduados en Electrónica, Computación, Información y Comunicaciones.

Este trabajo es requisito parcial para obtener el grado de Maestro en Administración de Telecomunicaciones.

INSTITUTO TECNOLÓGICO Y DE ESTUDIOS SUPERIORES DE MONTERREY

DICIEMBRE 2005

Dedicatoria

A Dios

Esta tesis se la dedico primeramente a Dios, ya que sin Él nada podemos hacer. Dios es quien nos concede el privilegio de la vida y nos ofrece lo necesario para lograr nuestras metas. Señor, GRACIAS, Gracias de todo corazón por permitirme estar aquí, por las pruebas que me hacen crecer como persona y ser humano y me permiten dar lo mejor de mí.

A mis padres:

Por todo el amor y apoyo que juntos me han dado. Porque nunca me dejaron solo y siempre han estado ahí en las buenas y en las malas. Y porque Ustedes dos han dado lo mejor de cada uno para que mis logros se realizaran. Por sus sabios consejos en el momento oportuno. Los amo.

Agradecimientos

A mi asesor

Por ser un excelente guía y persona. Y sobre todo, por la paciencia y por su constante apoyo en este proyecto.

Resumen

Las empresas enfrentan tiempos en los que la información es mucho más vulnerable, debido a la tecnología y al creciente número de ataques y vulnerabilidades de los sistemas de información.

Las personas juegan un papel fundamental en la seguridad de la información, no solo en el sentido de la protección de la misma, sino por representar el factor más importante de incidentes dentro de las organizaciones.

En este documento se presenta un modelo, en el cual, se representa el papel que juegan las personas en un sistema de seguridad de información simulado. Esta representación de las personas se da en base a las siguientes variables: "Percepción de Riesgo", "conformidad" y "BBP" (distribución preferida de actividades de seguridad).

Estas variables son los factores humanos de mayor riesgo causantes de un 80 a un 90 por ciento de todos los incidentes causados dentro de una organización. Lograr controlar estos factores, sería fundamental en la seguridad de una organización; ya que se lograría poder mantener la seguridad dentro de un nivel óptimo, o poder disminuir la frecuencia con la que se presentan los incidentes de seguridad.

Una herramienta que utilizaremos para poder influir y controlar estos factores humanos es el "Condicionamiento Instrumental", ya que nos permitirá entender el comportamiento humano y nos dará la técnica para poder influir en él.

Uno de los criterios de aplicación del condicionamiento instrumental es que, los incidentes de seguridad ejercen este mismo tipo de condicionamiento sobre el comportamiento humano, incrementando la percepción del riesgo y el incremento del nivel se seguridad. Intentaremos copiar el efecto que los incidentes causan sobre los factores humanos y disminuir los efectos contrarios causados por los espaciados tiempo sin incidentes, la mala percepción del riesgo real.

El condicionamiento instrumental, aplicado de manera constante e ininterrumpida, permitirá que el BBP cambie, ya que a largo plazo se empieza a dar un aprendizaje (en este caso, un cambio en el comportamiento del BBP).

En las simulaciones se ha demostrado que, si el BBP incrementa, el nivel de seguridad en el sistema se mantiene en un nivel de seguridad óptimo, aunque el nivel de percepción del riesgo decaiga.

Este trabajo esta basado en ecuaciones y ejemplos puramente teóricos, los cuales se emplean para ejemplificar la realidad de seguridad en las organizaciones.

Índice de Contenido

Dedicatoria iii
Agradecimientos iv
Resumen v

CAPITULO 1: INTRODUCCIÓN 1

1.1.- INTRODUCCIÓN 1
1.2.- JUSTIFICACIÓN 2
1.3.- OBJETIVOS 3
1.4.- APORTACIÓN 4

CAPÍTULO 2: ANTECEDENTES 5

2.1.- SÍNTESIS 5
2.2.-SEGURIDAD 5
2.2.1.- LA SEGURIDAD DE LA INFORMACIÓN 5
2.2.2.- LOS RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN 7
2.3.- EL FACTOR HUMANO 7
2.4.- LOS ATAQUES INTERNOS 8
2.5.- POSIBLES EFECTOS DE UN ATAQUE A LA INFORMACIÓN. 9
2.6.- MOTIVOS PARA ATACAR LOS SISTEMAS DE INFORMACIÓN. 10

CAPÍTULO 3: MARCO TEÓRICO 11

3.1.- SÍNTESIS 11
3.2.- LOS SISTEMAS 11
3.3.- PENSAMIENTO SISTÉMICO 13
3.3.1.- PRINCIPIOS DEL PENSAMIENTO SISTÉMICO. 13
3.3.2.- LEYES DEL PENSAMIENTO SISTÉMICO 14
3.4.- DINÁMICA DE SISTEMAS 15
3.4.1.- MÉTODO PARA LA CREACIÓN DE MODELOS DE DINÁMICA DE SISTEMAS 16
3.5.- LOS MODELOS 17
3.6.- MODELOS DE SEGURIDAD 18
3.7.- MODELOS DE SEGURIDAD BASADOS EN LA DINÁMICA DE SISTEMAS. 20
3.8.- DESCRIPCIÓN DE LOS ASPECTOS GENERALES DEL MODELO. 20

CAPÍTULO 4: PROPUESTA 22

4.1.- SÍNTESIS 22
4.2.- MODELO PARTICULAR 22
4.3.- JUSTIFICACIÓN DE VARIABLES 25
4.4.- MÉTODO 28

4.4.1.- LA METODOLOGÍA A SEGUIR 28

CAPÍTULO 5: RESULTADOS 30

5.1.- SÍNTESIS 30
5.2.- RESULTADOS 30
5.2.1.- GRUPO DE PRUEBA 1 30
5.2.1.1.- Escenario 30
5.2.1.2.- Simulación 31
5.2.2.- GRUPO DE PRUEBA 2 33
5.2.2.1.- Escenario 33
5.2.2.2.- Simulación 33
5.2.3.- GRUPO DE PRUEBA 3 36
5.2.3.1.- Escenario 36
5.2.3.2.- Simulación 36

CAPÍTULO 6: CONCLUSIONES 38

6.1.- CONCLUSIONES 38
6.1.1.- DE LAS SIMULACIONES 38
6.1.2.- DE SEGURIDAD 38
6.2.- TRABAJOS FUTUROS 39

APÉNDICE A: DESCRIPCIÓN DE LAS VARIABLES DEL MODELO CAUSAL 40

APÉNDICE B: ECUACIONES DEL MODELO CAUSAL 42

APÉNDICE C: EJEMPLO DE APLICACIÓN DEL MODELO DE SEGURIDAD. 44

APÉNDICE D: SOFTWARE PARA LAS SIMULACIONES 46

BIBLIOGRAFÍA 47

Índice de Tablas

Tabla 1.- Efectos de los ataques. 9
Tabla 2.- Agentes agresores de la Información. 10
Tabla 3.- Motivos de ataques.. 10
Tabla 4- Diferentes tipos de modelos existentes. E.Prim (1998) 17

Índice de Gráficas

Gráfica 1.- Las gráficas a) y b) muestran el comportamiento del sistema con respecto al riesgo percibido, el riesgo actual y los ataques a la seguridad. 31
Gráfica 2.- Las gráficas a) y b) muestran la relación del incremento de la conformidad con respecto al nivel de seguridad. 32
Gráfica 3.- comportamiento de la conformidad y los niveles de seguridad. El aumento en tsk/da en el BBP se nota en el valor mínimo de la conformidad. Simulación propia. 34
Gráfica 4.- En ésta gráfica se muestran la relación entre la percepción de riesgo y la frecuencia de incidentes. Simulación propia 34
Gráfica 5.- Incremento de BBP a diferentes tasas a 10 años. Simulaciones propias 35
Gráfica 6.- comportamiento de la conformidad y los niveles de seguridad, cuando el BBP no incrementa y se mantiene con su valor inicial constante. Simulación propia. 36
Gráfica 7.- En ésta gráfica se muestran la relación entre el aumento de la percepción de riesgo y la disminución en la frecuencia de incidentes. Simulación propia..... 37

Índice de Figuras

Figura 1.- Modelo causal de seguridad. González (2002)..... 21
Figura 2.- Diagrama causal de la Seguridad de la Información con modificación en el BBP, la conformidad y la percepción de riesgo..... 23
Figura 3.- Secuencia de acción de las fases de condicionamiento y de reforzamiento. 25
Figura 4.- Grupo de variables del Reforzamiento Instrumental que actúan sobre el BBP..... 26
Figura 5.- Tiempo de decremento del nivel de conformidad. Gráfica tomada de González, (2002). 27

Índice de Tablas

Tabla 1.- Efectos de los ataques. 9
Tabla 2.- Agentes agresores de la Información. 10
Tabla 3.- Motivos de ataques.. 10
Tabla 4- Diferentes tipos de modelos existentes. E.Prim (1998) 17

Índice de Gráficas

Gráfica 1.- Las gráficas a) y b) muestran el comportamiento del sistema con respecto al riesgo percibido, el riesgo actual y los ataques a la seguridad. 31
Gráfica 2.- Las gráficas a) y b) muestran la relación del incremento de la conformidad con respecto al nivel de seguridad. 32
Gráfica 3.- comportamiento de la conformidad y los niveles de seguridad. El aumento en tsk/da en el BBP se nota en el valor mínimo de la conformidad. Simulación propia. 34
Gráfica 4.- En ésta gráfica se muestran la relación entre la percepción de riesgo y la frecuencia de incidentes. Simulación propia 34
Gráfica 5.- Incremento de BBP a diferentes tasas a 10 años. Simulaciones propias 35
Gráfica 6.- comportamiento de la conformidad y los niveles de seguridad, cuando el BBP no incrementa y se mantiene con su valor inicial constante. Simulación propia. 36
Gráfica 7.- En ésta gráfica se muestran la relación entre el aumento de la percepción de riesgo y la disminución en la frecuencia de incidentes. Simulación propia..... 37

Índice de Figuras

Figura 1.- Modelo causal de seguridad. González (2002)..... 21
Figura 2.- Diagrama causal de la Seguridad de la Información con modificación en el BBP, la conformidad y la percepción de riesgo..... 23
Figura 3.- Secuencia de acción de las fases de condicionamiento y de reforzamiento. 25
Figura 4.- Grupo de variables del Reforzamiento Instrumental que actúan sobre el BBP..... 26
Figura 5.- Tiempo de decremento del nivel de conformidad. Gráfica tomada de González, (2002). 27

Índice de Tablas

Tabla 1.- Efectos de los ataques. 9
Tabla 2.- Agentes agresores de la Información. 10
Tabla 3.- Motivos de ataques.. 10
Tabla 4- Diferentes tipos de modelos existentes. E.Prim (1998) 17

Índice de Gráficas

Gráfica 1.- Las gráficas a) y b) muestran el comportamiento del sistema con respecto al riesgo percibido, el riesgo actual y los ataques a la seguridad. 31
Gráfica 2.- Las gráficas a) y b) muestran la relación del incremento de la conformidad con respecto al nivel de seguridad. 32
Gráfica 3.- comportamiento de la conformidad y los niveles de seguridad. El aumento en tsk/da en el BBP se nota en el valor mínimo de la conformidad. Simulación propia. 34
Gráfica 4.- En ésta gráfica se muestran la relación entre la percepción de riesgo y la frecuencia de incidentes. Simulación propia 34
Gráfica 5.- Incremento de BBP a diferentes tasas a 10 años. Simulaciones propias 35
Gráfica 6.- comportamiento de la conformidad y los niveles de seguridad, cuando el BBP no incrementa y se mantiene con su valor inicial constante. Simulación propia. 36
Gráfica 7.- En ésta gráfica se muestran la relación entre el aumento de la percepción de riesgo y la disminución en la frecuencia de incidentes. Simulación propia..... 37

Índice de Figuras

Figura 1.- Modelo causal de seguridad. González (2002)..... 21
Figura 2.- Diagrama causal de la Seguridad de la Información con modificación en el BBP, la conformidad y la percepción de riesgo..... 23
Figura 3.- Secuencia de acción de las fases de condicionamiento y de reforzamiento. 25
Figura 4.- Grupo de variables del Reforzamiento Instrumental que actúan sobre el BBP..... 26
Figura 5.- Tiempo de decremento del nivel de conformidad. Gráfica tomada de González, (2002). 27

Capítulo 3: Marco Teórico

3.1.- Síntesis

La Dinámica de Sistemas es una metodología para la construcción de modelos de simulación para sistemas complejos que se basa en la utilización del enfoque del pensamiento sistémico.

El pensamiento sistémico implica una visión de la realidad compleja en sus múltiples elementos y con sus diversas interrelaciones. Esto es simplemente el reconocimiento de la naturaleza sistémica del mundo. Sin embargo en la práctica no es tan sencillo como parece.

Para tomar decisiones bajo este enfoque debemos conocer íntegramente el sistema.

Esto nos abre la pauta para comenzar este capítulo hablando a cerca de los sistemas, explicando los tipos de sistemas que existen, los elementos que los conforman y sus comportamientos.

Así mismo, para poder entender con mayor claridad a los modelos de seguridad, hablaremos de los modelos, los diferentes tipos que existen, sus utilidades y las ventajas que de ellos obtenemos.

Ya al final del capítulo englobaremos los conceptos de "pensamiento sistémico", "dinámica de sistemas" y los "modelos de seguridad", para explicar a los Modelos de seguridad basados en la Dinámica de sistemas.

3.2.- Los sistemas

Para poder entender con mayor claridad el "Pensamiento Sistémico" y la "Dinámica de Sistemas" es necesario entender primero a los sistemas, los tipos de sistemas, sus características, comportamientos y los elementos que los conforman, ya que de ellos se basan estos métodos.

Comenzaremos describiendo a un sistema como una unidad cuyos elementos interaccionan juntos, ya que continuamente se afectan unos a otros; de modo que operan hacia una meta común, (Instituto Tecnológico de Sonora, [ITSON], s.f.).

Los sistemas se perciben con una identidad que los distinguen de lo que los rodea y que son capaces de mantener a lo largo del tiempo y bajo entornos cambiantes.

Según V. Anderson et al (1977), los sistemas se pueden separar en dos grupos.

- **Sistemas Naturales:** el cuerpo de un ser viviente, las sociedades humanas, un ecosistema; los cuales tienen un gran número de componentes con una gran complejidad de interrelaciones entre esos componentes. También tienen un número infinito de conexiones con los sistemas que los rodean.

- **Sistemas No vivientes (Hechos por el hombre):** las interacciones de una compañía, los cuales pueden ser también bastante complejos.

Los sistemas existentes por el comportamiento que se ve a través del tiempo como:

- **Sistemas Dinámicos:** Es el que muestra cambios en su estructura o en las relaciones entre sus elementos a través del tiempo.

- **Sistema Estático:** es aquel cuya estructura y relaciones entre sus elementos puede considerarse permanentes a través del tiempo.

Las características esenciales de los sistemas son:

1. Las partes de los sistemas deben estar todas presentes para que el sistema realice se propósito de manera óptima.

2. Las partes de un sistema se deben arreglar de una manera específica para que el sistema realice su propósito.

3. Los sistemas tienen propósitos específicos dentro de un sistema mayor.

4. Los sistemas mantienen su estabilidad por medio de fluctuaciones y ajustes.

5. Los sistemas tienen retroalimentación.

Los elementos que conforman los sistemas pueden ser objetos físicos o intangibles.

- **Componentes Tangibles:** Computadoras, equipos de comunicaciones, servidores, equipos de vigilancia, etc.

- **Componentes Intangibles:** Flujos de información, interacciones interpersonales, estados interno de la mente, sentimientos, valores, creencias.

Resumiendo, los aspectos fundamentales del concepto Sistema son:

- La existencia de elementos diversos e interconectados.
- El carácter de unidad global del conjunto.
- La existencia de objetivos asociados al mismo.
- La integración del conjunto en un entorno.

3.3.- Pensamiento sistémico

El pensamiento sistémico es una metodología capaz de cubrir las situaciones y requerimientos para la resolución de problemas, la toma de decisiones y la planeación e implementación de estrategias en ambientes de gran escala y complejidad, con el alcance y los recursos necesarios para tratarlas adecuadamente.

El pensamiento sistémico nos proporciona un análisis con un enfoque al todo, y no reduccionista, lo cual es ideal para entender el modelo del sistema de seguridad, que tiene un gran número de componentes con una gran complejidad de interrelaciones entre ellos mismos.

3.3.1.- Principios del pensamiento sistémico.

- Pensar con una visión más amplia: Implica dar un paso atrás del acontecimiento y mirarlo con una visión más amplia.

- Balancear las perspectivas a corto plazo y a largo plazo: el pensamiento sistémico muestran que los comportamientos que conducen al éxito a corto plazo afectan el éxito de acciones a largo plazo.

- Reconocer la naturaleza dinámica, compleja e interdependiente de los sistemas: si vemos al mundo de manera sistémica, vemos que todo es dinámico, complejo e interdependiente.

- Consideras factores cuantitativos y cualitativos: el pensamiento de sistemático fomenta el uso de datos cuantitativos y cualitativos. Ninguno de los dos es mejor, ambos son importantes y complementarios.

- Recordar que somos parte de los sistemas y que cada uno influimos en él, incluso mientras somos influenciados por el sistema mismo: uno de los principios más

retadores del pensamiento sistémico es que nosotros mismos contribuimos a nuestros propios problemas.

3.3.2.- Leyes del Pensamiento Sistémico

De acuerdo con Senge (1993), las bases del pensamiento sistémico son las once leyes que a continuación se establecen:

1. Los problemas de hoy provienen de las soluciones de ayer
2. Cuanto más se presiona al sistema, este más reacciona
3. El comportamiento mejora antes de empeorar
4. El camino fácil usualmente lleva al mismo lugar
5. La cura puede ser peor que la enfermedad
6. Cuanto más rápido se avance, más lento se llega
7. La causa y efecto no están necesariamente relacionado en tiempo y espacio.
   a. Si hay un problema en un departamento se busca la causa solo en ese departamento y no en otra sección o en otro momento
8. Pequeños cambios producen grandes resultados
   a. La introducción de un sistema de correo electrónico en una organización puede crear enormes cambios en los procedimientos de comunicación de toda la empresa.
9. Se puede cortar el pastel y comerlo, pero no todo al mismo tiempo
   a. Pretender implementar programas de bajo costo y alta calidad al mismo tiempo y en forma instantánea, y querer tener resultados positivos.
   b. No se puede tomar la foto y ver lo que esta ocurriendo al mismo tiempo.
10. Dividir al elefante no produce elefantitos
   a. Divide y vencerás. Al dividir el problema de la comunicación dentro de la organización se cree que es posible resolverlo, (equivocación total)

11. No hay culpas

    a. Todas las partes son responsables del problema

Visto como un lenguaje, el pensamiento sistémico tiene características únicas que lo hacen ser una herramienta de valor para tratar temáticas de sistemas complejos.

- Se enfatiza en ver los "todos en vez de las partes y enfatiza el papel de las interconexiones. Lo más importante es que se reconoce que somos parte del sistema en el cual funcionamos y por eso, contribuimos en el comportamiento de los mismos.

- En un lenguaje circular más que lineal, se centra en las interdependencias cerradas, donde x influye en y, y influye en z, y z regresa en influye en x.

- Tiene un conjunto de reglas precisas que reduce la ambigüedad y los malos entendidos que pueden surgir cuando se habla de situaciones complejas.

- Ofrece herramientas visuales como diagramas causales y gráficas de comportamiento sobre el tiempo. Estos diagramas son ricos para mostrar implicaciones y consecuencias, permitiendo un mejor entendimiento. Hacen énfasis en la dinámica del problema y no en las culpas individuales.

- Abre una ventana nueva en nuestros esquemas mentales, traduciendo nuestras percepciones individuales a imágenes explicitas que pueden dejar ver diferencias significativas en puntos de vista ligeramente distintos.

3.4.- Dinámica de Sistemas

Las interrelaciones de la tecnología, el entorno de trabajo y el comportamiento humano en cuestiones de seguridad, forman un sistema caracterizado por retroalimentaciones, cambios temporales, retardos, y aspectos interdisciplinarios, (González, 2002).

Para poder estudiar y entender esas relaciones necesitamos una metodología que esté diseñada para manejar todos estos factores.

J. Forrester, (1961), describe la Dinámica de Sistemas como una metodología para estudiar y administrar sistemas complejos de retroalimentación, tales como los que se encuentran en las organizaciones y otros sistemas sociales; por lo tanto, la Dinámica de Sistemas es una excelente herramienta para:

a) comprender cómo son las estructuras que producen determinados comportamientos.

b) expandir nuestra concepción de las interrelaciones que gobiernan los procesos de cambio.

c) imaginar escenarios.

d) diseñar estrategias que faciliten la toma de decisiones.

Jay W. Forrester del M.I.T. (Massachusetts Institute of Technology) desarrolló esta metodología durante la década de los cincuenta. Los fundamentos técnicos y filosóficos de la dinámica de sistemas se encuentran en la simulación analógica de teoría de control y el pensamiento sistémico, respectivamente, (Grupo de Modelación Dinámica de Sistemas, 2002).

La dinámica de sistemas, permite ir más allá de los estudios de casos y las teorías descriptivas; no está restringida a sistemas lineales, pudiendo hacer pleno uso de las características no-lineales de los sistemas. Combinando estas características con un buen software, los modelos de dinámica de sistemas permiten una simulación eficaz de sistemas complejos. Dicha simulación representa la única forma de determinar el comportamiento en los sistemas no-lineales complejos, (J. Forrester, 1964).

Esta técnica muestra cómo van cambiando las cosas a través del tiempo. Un proyecto de dinámica de sistemas comienza con un problema que hay que resolver en un comportamiento indeseable que hay que corregir o evitar dentro de un sistema, (J. Forrester, 1964).

La dinámica de sistemas usa conceptos del campo del control retroalimentado para organizar información en un modelo de simulación por computadora. Un software ejecuta los papeles de los individuos en el mundo real; la simulación resultante revela implicaciones del comportamiento del sistema representado por el modelo, (Grupo de Modelación Dinámica de Sistemas, 2002).

Al hablar de la dinámica de un sistema nos referimos a que las distintas variables que podemos asociar a sus partes, sufren cambios a lo largo del tiempo como consecuencia de las interacciones que se producen en ellas. Su comportamiento vendrá dado por el conjunto de trayectorias de todas las variables, que suministra algo así como una narración de lo acontecido en el sistema, (J. Forrester, 1961).

3.4.1.- Método para la creación de modelos de dinámica de sistemas

El método empieza con la identificación de la situación problemática y el propósito del modelo. Termina con el diseño de una solución o implantación de cambios en alguna política de la empresa. Los pasos a seguir son, (Vennix, 1996):

1. Identificación del problema y propósito del modelo.

2. Conceptualización del sistema.

3. Formulación del modelo y estimación de parámetros.

4. Análisis del comportamiento del modelo.

5. Evaluación del modelo.

6. Uso del modelo o implantación.

3.5.- Los modelos

Ya que la Dinámica de Sistemas emplea los modelos, es necesario entender los; los diferentes tipos de modelos que existen, sus utilidades y ventajas.

Según E. Prim (1998), los modelos son versiones simplificadas de la realidad, que son utilizadas para estudiar y en tender problemas tan complicados y complejos de la vida real.

E. Prim (1998) definió en su libro que un modelo es una simplificación que imita los fenómenos del mundo real, de modo que se puedan comprender las situaciones complejas y podamos hacer predicciones

MODELO	DESCRIPCIÓN
Verbales	Es un modelo simple como una explicación con palabras de lo fundamental de una realidad, del funcionamiento de un sistema fácil de entender.
Gráficos	Modelos que utilizan diagramas en los que se dibujan, de una forma simplificada, los componentes del sistema señalando con flechas las acciones de unos sobre otros.
Numéricos	Modelos en los que se utilizan magnitudes y ecuaciones matemáticas para describir con exactitud los distintos componentes del sistema y las relaciones entre ellos.
Computacionales	El desarrollo de computadoras ha hecho posible manejar una gran cantidad de datos, en los que con software se imita el funcionamiento de sistemas complejos.

Tabla 4- Diferentes tipos de modelos existentes. E.Prim (1998)

Los modelo permiten predecir situaciones futuras porque como imita la realidad da la posibilidad de adelantarse al presente y situarse en lo que vendrá E.Prim (1998)

E.Prim (1998) menciona que otra ventaja de los modelos es que permiten hacer "experimentos" que nunca serían posibles en la realidad. La limitación obvia es que un modelo imita, por lo tanto, no es la realidad. Y dado esto, por muy bueno que sea siempre estará lejos de la complejidad de los procesos naturales.

3.6.- Modelos de Seguridad

Un modelo de seguridad proporciona una representación que describe las propiedades funcionales y estructurales de la seguridad de nuestro sistema. Permite a los desarrolladores trabajar con una definición de alto nivel de los requerimientos de protección y las políticas de seguridad así como producir una descripción concisa y precisa del comportamiento esperado del sistema, (Políticas y Modelos de seguridad, s.f.).

|Las características del modelo que escojamos para expresar los requerimientos deben ser:

- Fácil de comprender.
- Implementable.
- Carente de ambigüedad.
- Capaz de incorporar las políticas de la compañía.

En la actualidad existen diferentes tipos de modelos de seguridad, cada uno da solución a diferentes tipos de necesidades de los usuarios. Existen esquemas que se basan en la integridad de la información, otros esquemas se basan en la autenticación de los usuarios del sistema y otros tantos se basan en la privacidad de la información, (C. Arellano et al, s.f.).

- Modelos basados en el control de acceso por role (RBAC Role Based Access Control).
- Modelo basado en la separación de tareas (SoD Separation of Duties). La separación física y lógica de tareas puede mejorar la prevención de actividades no autorizadas.

Los principales modelos existentes contemplan, como principal preocupación, el control de acceso y la integridad; modelos como los utilizados por los productos de Microsoft, implementan una seguridad y control de cambios para sus documentos basados en autentificación de usuario, este puede proteger sus documentos y conocer la identidad de los usuarios que realizan cambios sobre un documento, pero no le asegura que el

documento no sufrió modificaciones en el transcurso del proceso de colaboración, (C. Arellano et al, s.f.).

En esquemas de seguridad generales los modelos deben contemplar los siguientes aspectos:

- Proteger los datos para que no puedan ser leídos o modificados por personas que no tienen autorización para hacerlo.
- Impedir que las personas sin autorización inserten o borren información.
- Verificar al emisor e incluso al receptor de la información.
- Hacer posible que los usuarios transmitan electrónicamente documentos firmados.

Para dar solución a estas necesidades los modelos de seguridad deben proponen opciones de implementación que aseguren estos tres aspectos básicos de la información:

a) Confidencialidad

b) Integridad.

c) .Disponibilidad

Todo lo anterior soportado por políticas definidas para cada una de las necesidades de seguridad y por mecanismos que logren generar un esquema de trabajo seguro (C. Arellano et al, s.f.).

Es muy importante comprender que el comportamiento que se proponga para el sistema en cuanto a seguridad se verá fuertemente influenciado por las amenazas que el sistema debe afrontar y del tipo de sistema en el que se apliquemos. Es muy diferente plantear un modelo para un entorno de alta seguridad, en el cual, la mayor preocupación sea la posible filtración de información confidencial, en contraste con un entorno comercial, más preocupado por asegurar la integridad y actualidad de la información. Son estos tipos de detalles los que nos guiarán a la hora de elegir el modelo, (Políticas y Modelos de seguridad, s.f.).

3.7.- Modelos de Seguridad basados en la Dinámica de Sistemas.

Los modelos de seguridad basados en la dinámica de sistemas, proporcionan una representación que describe las propiedades funcionales y estructurales de la seguridad de un sistema. Muestra las interrelaciones de la tecnología, el entorno de trabajo y el comportamiento humano; en un sistema caracterizado por retroalimentaciones, cambios temporales, retardos, y aspectos interdisciplinarios. Además se basa en una metodología capaz de cubrir las situaciones y requerimientos para la resolución de problemas, toma de decisiones y la planeación e implementación de estrategias en ambientes de gran escala y complejidad.

Este tipo de modelos, al basarse en la Dinámica de sistemas, que a su vez se sustenta en la metodología del Pensamiento Sistémico y aunado a las características de los modelos, les da todas las ventajas y características de cada uno de los métodos mencionados.

Los modelos basados en la dinámica de sistemas nos permitirán ver los cambios que van sufriendo las variables a lo largo del tiempo como consecuencia de las interacciones que se producen en ellas, (J. Forrester, 1961). Estos cambios sufridos por las variables a lo largo del tiempo se visualizan a través de los softwares de simulación, los cuales permiten revelar las implicaciones del comportamiento del sistema representado por el modelo, (Grupo de Modelación Dinámica de Sistemas, 2002).

De a cuerdo con González (2002), estos tipos de modelos basados en la Dinámica de Sistemas, nos permitirá mejorar la robustez de los sistemas modernos de seguridad e incrementar el entendimiento del rol de los factores humanos. Así, lograr el más alto objetivo que es ganar entendimiento de las relaciones intrínsecas entre las personas, la tecnología y en ambiente de trabajo en los sistemas de seguridad.

3.8.- Descripción de los aspectos generales del modelo.

Para poder entender con claridad la investigación en esta tesis, es importante describir el funcionamiento del modelo presentado por González (2002).

Los “Riesgos Internos y Externos” describe el patrón de incidentes durante un período de tiempo. Esta variable, afecta directamente a la variable “Nivel de seguridad Prescrito”, la cual están indicadas por las políticas de seguridad de la organización. A medida que aumenta la variable “Riesgos Internos y Externos”, aumenta el “Nivel de seguridad Prescrito” y el “Riesgo Actual”.

La percepción del riesgo, definida en el modelo como “Riesgo Percibido”, va variando gradualmente a través del tiempo. Esta variable describe la percepción del riesgo en el sistema.

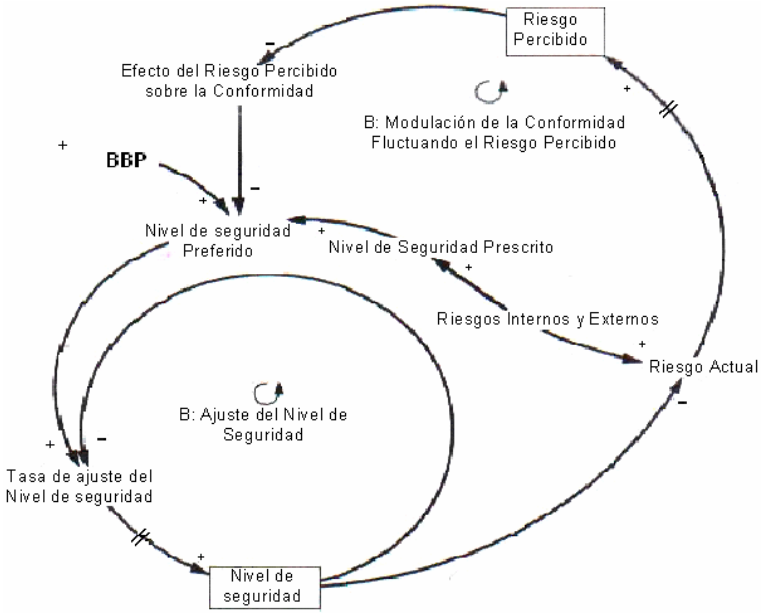


Figura 1.- Modelo causal de seguridad. González (2002).

Esta variable es modificada por dos fuerzas condicionadotas; una positiva que aumenta la percepción del riesgo en el sistema, representada por los incidentes de seguridad, y otra negativa que decrementa la percepción del riesgo, dada por los períodos de tiempo en los que no se presentan incidentes de seguridad. Estos procesos son llevados a cabo en el tiempo y se representa en el modelo por las dos líneas cruzadas sobre las líneas de influencia de "Riesgo Actual" hacia "Riesgo Percibido".

La variable "Riesgo Percibido" modula a la conformidad a través de la variable "Efecto del riesgo percibido en la conformidad"), que representa la variación de la conformidad que se tiene con el "Nivel de seguridad Prescrito". Esto es: una percepción de riesgo baja, dará por resultado que el "Nivel de seguridad Preferido"="BBP". Y por el contrario, una percepción de riesgo alta dará por resultado que el "Nivel de seguridad Preferido"= "Nivel de seguridad Prescrito"

La variable "Nivel de seguridad", es un almacenador, que va variando a través del tiempo de manera gradual por medio de flujos. Si el valor de "Nivel de seguridad Preferido" es mayor que el valor actual del "Nivel de seguridad", esta variable es incrementada, describiendo el efecto del Condicionamiento Instrumental producido por una percepción del riesgo alta. Por el contrario, si el valor de "Nivel de seguridad Preferido" es menor que "Nivel de seguridad", el valor de ésta variable decrementa por el efecto de la extinción del condicionamiento (retorno al "Nivel de seguridad"="BBP").

Las ecuaciones que describen el modelo a bloques se encuentra en el Apéndice B

Capitulo 1: Introducción

1.1.- Introducción

Preservar la confidencialidad, integridad y disponibilidad de la información, se ha convertido en una tarea fundamental de la seguridad dentro de una organización; ya que ésta es el principal recurso, necesario para lograr los objetivos económicos y sociales de la organización.

Son comunes los esquemas de seguridad en las organizaciones, en los cuales, se protegen a estas de incidentes externos. Éstas organizaciones se encuartelan instalando sistemas modernos de seguridad en sus redes de datos, de vigilancia y de acceso a sus instalaciones, lo cual, les crea un alto grado de percepción de seguridad dentro de la organización, perdiendo de vista el riesgo real.

El enfocarse a aspectos externos y no tomar en cuenta un factor muy importante como el humano, hace que los sistemas sean vulnerables y muy susceptibles a fallos de seguridad. Dado que no existe sistema informático alguno al que no dependa de operadores humanos, estos se vuelven centro de a ataques internos, poniendo en jaque a toda la organización.

En esta investigación se presenta un modelo de seguridad basado en la dinámica de sistemas, en el cual se integran el entorno de trabajo, la tecnología y el comportamiento humano, como los tres principales factores que interaccionan dentro de la seguridad en una organización.

Este modelo, que aplica la metodología del pensamiento sistémico, la cual nos proporciona una visión conjunta, que nos permitirá configurar la seguridad de la organización mediante procesos definidos y aplicables.

Esta metodología es capaz de cubrir las situaciones y requerimientos para la resolución de problemas, la toma de decisiones y la planeación e implementación de estrategias en ambientes de gran escala y complejidad, con el alcance y los recursos necesarios para tratarlas adecuadamente. Es ideal para entender el modelo del sistema de seguridad, que tiene un gran número de componentes con una gran complejidad de interrelaciones entre ellos mismos.

La tesis se centra en el comportamiento humano como factor de mayor riesgo a la seguridad de la información dentro de la organización.

La percepción de riesgo, la conformidad con los niveles de seguridad y la distribución preferida de actividades de seguridad, son comportamientos humanos; y por ende, necesitamos una herramienta la cual nos ayude a comprender e influir en ellos.

Se propone la utilización del condicionamiento instrumental como medio para poder entender el comportamiento y la técnica para influir en él.

El condicionamiento instrumental, nos servirá como medio para reforzar el comportamiento que resulta después de un incidente de seguridad. Ya que de las simulaciones se ha podido apreciar que los niveles de seguridad se incrementan a través del condicionamiento que los incidentes ejercen sobre la percepción de riesgo y la conformidad.

La distribución preferida de actividades de seguridad, no se ve afectada por estos condicionamientos que ejercen los incidentes, ya que la única manera de que fuera modificada, sería que existiera un aprendizaje; y dado que los incidentes están muy espaciados en tiempo y no son continuos, no son suficientes como para modificar este comportamiento.

El condicionamiento instrumental aplicado como reforzamiento a la respuesta instrumental causada por los incidentes de seguridad, puede permitir el aprendizaje de nuevos niveles de seguridad en el comportamiento, si son aplicados de manera continua e ininterrumpida y de manera constante.

Los resultados obtenidos de las simulaciones, ayudarán a la toma de decisiones y formulación de políticas de seguridad.

Los resultados son presentan tres grupos de simulaciones. En los dos primeros se analiza el comportamiento del sistema después de aplicado el condicionamiento instrumental, pero en el primer grupo, los incrementos en las variables que controlan el tiempo de disminución de la percepción de riesgo y la conformidad con los niveles de seguridad, se dan en un solo tiempo, también los incrementos en la distribución preferida de actividades de seguridad se incrementa en un solo paso. En el segundo grupo de simulación, los incrementos de esas variables se dan en tasas de incrementos diarios. En el tercer grupo de simulación, la los incrementos de las variables que controlan el tiempo de disminución de la percepción de riesgo y la conformidad con los niveles de seguridad se dan con las mismas tasas de incremento diarias, pero con la diferencia de que la distribución preferida de actividades de seguridad no cambia de su valor inicial.

1.2.- Justificación

Se dice que el factor humano es el Talón de Aquiles de la seguridad de la información, ya que juega una parte muy esencial en la seguridad, ya que no existe sistema informático que no dependa de algún tipo de dato ingresado por algún operador humano, (González, 2002; Caruana, 2002).

Un problema en la percepción del riesgo es que se piensa que al contar con la tecnología de punta para la protección de la información y que se controlen los accesos a los servicios de la empresa, se estará totalmente protegido. Schneier B. (2002), en su libro “Secrets and

lies: Digital Security in a Networked World", dijo: "Si tu piensas que la tecnología puede resolver tus problemas de seguridad, entonces tu no entiendes los problemas y tu no entiendes la tecnología".

En un principio las empresas consideraban que tenían que protegerse de los agentes y ataques externos; pero con el paso del tiempo, las organizaciones han advertido que no sólo existen este tipo de amenazas, sino que también hay peligros dentro de la organización, y que éstos deberían ser contemplados a la hora de proteger la información.

Actualmente se sabe mucho a cerca de seguridad de redes y computadoras, pero no se tienen conocimientos suficientes para poder ayudar a resolver el verdadero problema que representa el factor humano.

Esto nos indica que el peligro no solamente esta en el exterior de la organización; ya que los mismos sistemas de seguridad internos son operados por humanos, podríamos pensar y estaríamos en lo correcto, de que la mayor cantidad de ataques, intencionados o no, se encuentran en el interior de la organización. M. Sisk (2005) dijo en una frece que suena a película de terror, "el enemigo está dentro".

M. Sisk (2005) indica que las evidencias en problemas de seguridad de la información están demostrando que las amenazas externas son solo una porción y no es la mayor de las amenazas a la seguridad de la información más preciada por las organizaciones. Una encuesta reciente del instituto de Ponemon de compañías financieras y no financieras, revelo recientemente que el 69 por ciento reporto serias fugas de datos debido a los errores malintencionados o no malintencionados de los empleados.

Los riesgos potenciales asociados con un ataque interno son mucho más altos hoy de lo que eran hace sólo unos años. Un ataque exitoso puede realmente detener a toda una compañía, (Microsoft, 2002).

A diferencia del atacante externo, los empleados de una empresa poseen conocimiento y disponen de mayores oportunidades para explotar vulnerabilidades existentes. Por esta razón, los ataques internos son altamente costosos y difíciles de identificar.

Por eso es importante tener el conocimiento de que los ataques internos representan una amenaza importante para las empresas, por ser éstos los causantes de daños patrimoniales significativos.

1.3.- Objetivos

- Lograr un entendimiento de las variables que intervienen en la seguridad organizacional, prestándole principal atención a las variables del comportamiento humano (percepción de riesgo, conformidad y distribución preferida de actividades de seguridad).

- Por medio del condicionamiento instrumental, explicar el comportamiento de las variables del comportamiento humano.

- Contribuir a un planteamiento de mejores políticas de seguridad de la información.

1.4.- Aportación

Esta tesis presenta un estudio del condicionamiento instrumental empleado como una herramienta para poder controlar y modificar factores de riesgos dentro de un modelo de seguridad de la información, representados por las variables del comportamiento humano.

Con este estudio se logra avanzar en el entendimiento del comportamiento humano con respecto a la percepción de los riesgos dentro y fuera de la organización, la conformidad con los niveles de seguridad y la distribución preferida de actividades de seguridad; Logrando con esto, mejorar el diseño y empleo de las políticas de seguridad.

Capítulo 4: Propuesta

4.1.- Síntesis

Los factores humanos representan los factores de mayor riesgo dentro de las organizaciones. Según Caruana, (2002), el factor humano es una parte esencial del juego de seguridad, ya que no existe un sistema informático que no dependa de algún dato ingresado por algún operador humano.

Dado que los factores humanos se ven involucrados en los problemas de seguridad de las organizaciones, esos problemas se vuelven complejos y dinámicos.

Los factores humanos son presentados en este capitulo a través de los conceptos de "percepción del riesgo", "conformidad" y "distribución preferida de actividades de seguridad".

Es importante aclarar que las ecuaciones que definen a las variables en el Apéndice B, son totalmente teóricas, al igual que los ejemplos.

4.2.- Modelo Particular

Para poder visualizar, de una manera global y experimentalmente, cómo se relacionan e interactúan el comportamiento humano, la tecnología y el entorno dentro de una organización con respecto a la seguridad, utilizaremos el modelo planteado por González (2002), descrito anteriormente.

El problema más fuerte que enfrentan las organizaciones con respecto a la seguridad, es que se acostumbran a su aparente seguridad. Este sentimiento de seguridad se ve respaldado por los avances de la tecnología y los periodos prolongados en los que no se presentan incidentes, permitiendo que las organizaciones se sientan fuera de peligro debido a la mala percepción del riesgo, (Swiss Re, 1998).

El "Riesgo Percibido" es un factor humano con el que se modela el comportamiento en un período de tiempo en que no se presentan incidentes de seguridad, donde se pierde de vista el riesgo real y es substituido por la percepción.

González (2002), indica que la percepción del riesgo es extremadamente volátil y depende directa o indirectamente de circunstancias tales como las experiencias propias o reportadas.

La percepción del riesgo es alta cuando ocurren incidentes de seguridad, ya que estos actúan como condicionadores naturales para la percepción del riesgo. Con el paso del tiempo esta percepción va disminuyendo debido a los periodos de tiempo largos en los que no se presentan incidentes; esta ausencia de los reforzadores naturales (incidentes), y la sobre-confianza en la tecnología, conlleva a una mala percepción del riesgo con la consecuente disminución de la conformidad.

La "conformidad" es la aceptación de los niveles de seguridad establecidos por las políticas de seguridad de la organización, indicadas por la variable "nivel de seguridad prescrito". A medida que la "conformidad" decrementa, el nivel de seguridad también disminuye con el.

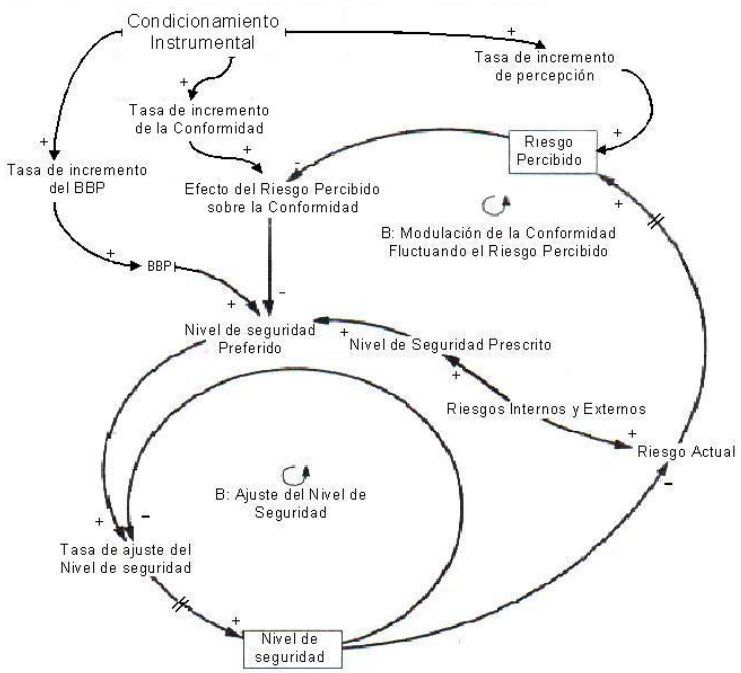


Figura 2.- Diagrama causal de la Seguridad de la Información con modificación en el BBP, la conformidad y la percepción de riesgo.

Esto se puede apreciar en el modelo a través de los lazos de retroalimentación de balance (B: balance). El lazo negativo de retroalimentación llamado "modulación de la conformidad fluctuando el riesgo percibido", muestra como la Percepción del Riesgo va modulando a la conformidad con respecto al tiempo. De acuerdo a la percepción del riesgo, la conformidad va aumentando o disminuyendo, lo cual afecta al nivel de seguridad. El segundo lazo negativo de retroalimentación llamado "Ajuste del nivel de seguridad" nos muestra como los niveles de seguridad se retroalimentan de acuerdo a la conformidad.

El nivel más bajo de seguridad se presenta al entrar en un estado de relajación, en este punto la conformidad prácticamente es nula y da paso a la distribución preferida de actividades de seguridad "BBP".

Este estado de relajación se da cuando la percepción del riesgo es casi nula y además reforzada por el sentimiento de seguridad dado por los avances de la tecnología y los periodos prolongados en los que no se presentan incidentes.

El Behavioral Bliss Point (BBP) es el Punto de Satisfacción del la Conducta; esto puede entenderse como la cantidad de tareas de seguridad que el individuo esta acostumbrado a realizar. Cuando una persona esta acostumbrado a realizar una tarea con una cierta frecuencia se dice que ese esa frecuencia es su BBP. Cuando se cambia esa frecuencia debido a políticas de seguridad que indiquen realizar con una frecuencia mayor que la que se esta acostumbrado, se requiere estar en conformidad con dicha frecuencia de las tareas a ejecutarse, de manera contraria, la frecuencia de ejecución de las tareas de seguridad volverán a establecerse en el BBP.

Con la aparición del BBP, el nivel de seguridad ya no estará dictado por las políticas de seguridad, sino por la propia distribución preferida de actividades de seguridad del BBP.

El efecto de la disminución de la conformidad originado por la percepción errónea del riesgo y la aparición consecuente del BBP, son aspectos del modelo que deseamos controlar. Para ello se propone el empleo del condicionamiento instrumental.

Los incidentes de seguridad tienen un efecto de condicionamiento instrumental sobre la percepción del riesgo y la conformidad. Ya que en una contingencia, la percepción del riesgo se incrementa, modulando la conformidad y elevando los niveles de seguridad.

Se propone utilizar el Condicionamiento Instrumental como medio de Reforzamiento a la respuesta causada por los incidentes de seguridad; para mantener la percepción del riesgo y la conformidad elevados.

M. Alexander, (2002), define al condicionamiento instrumental como "la ciencia de explicar el comportamiento y la técnica para cambiarlo". En esencia, ésto es lo que requerimos para entender los factores humanos de comportamiento dentro de una organización y poderlo controlar.

El condicionamiento instrumental opera en tres fases:

1. **EL ESTÍMULO** que provoca el comportamiento. (*incidentes*)

2. **EL COMPORTAMIENTO** de reacción de las personas. (*aumento de la percepción del riesgo y la conformidad*)

3. **LA CONSECUENCIA** ocurre como resultado del comportamiento (*aumento de los niveles de seguridad*)

Estas fases se tienen que repetir en un ciclo constantemente para mantener el nivel de seguridad del sistema. Dado que no esperamos repetir los incidentes de seguridad para mantener los niveles de seguridad elevados; lo haremos mediante el empleo del condicionamiento instrumental, que en este modelo funcionará como un reforzador de la respuesta instrumental *(aumento de la percepción del riesgo y la conformidad).*

Al condicionamiento instrumental le llamaremos "Reforzamiento Instrumental", ya este que reforzará el comportamiento producido por los incidentes de seguridad, como se ilustra en la figura 2.

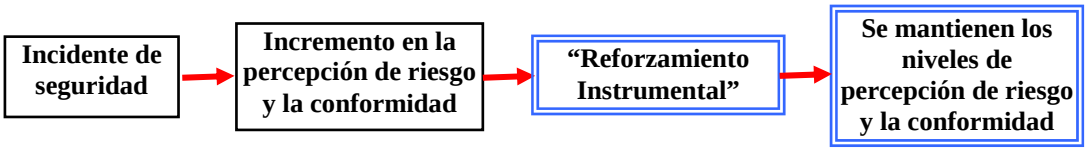


Figura 3.- Secuencia de acción de las fases de condicionamiento y de reforzamiento.

Al ser aplicado el condicionamiento instrumental en ciclos constantes, se influye también un cambio en el BBP. Esto debido a que el condicionamiento instrumental Influye en los cambios del comportamiento o aprendizaje. Es posible establecer la meta de ese aprendizaje, donde la meta podría ser el aumento del número de actividades de seguridad; en pocas palabras se diría que se hace un cambio de $BBP_1 \Rightarrow BBP_2$, donde BBP_2 es mayor que BBP_1

$$\text{Comportamiento} \Rightarrow \text{Recompensa} \Rightarrow \text{Aprendizaje}$$

Donde;

- **Comportamiento**: aceptación de los niveles de seguridad.
- **Recompensa**: mayor seguridad.
- **Aprendizaje**: Cambio en el BBP.

4.3.- Justificación de Variables

El "Reforzamiento Instrumental" esta compuesto de tres variables "Número mínimo de sesiones de reforzamiento instrumental al año", "Sesiones de reforzamiento instrumental programadas al año" y "Determinador del reforzamiento Instrumental".

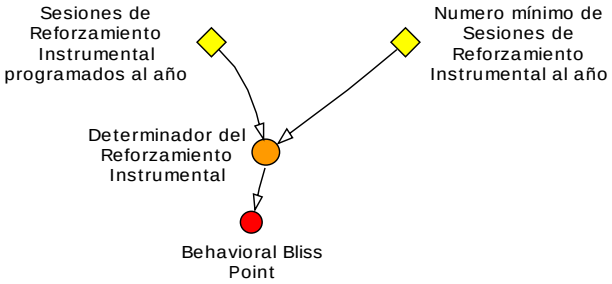


Figura 4.- Grupo de variables del Reforzamiento Instrumental que actúan sobre el BBP. Tomadas del modelo a bloques.

Estas variables, reforzarán el condicionamiento causado por los incidentes se seguridad que se hayan presentado en la organización, de tal manera que actuarán como sensibilizadores, los cuales modificarán el comportamiento de las personas hacia la percepción de riesgo.

El reforzamiento debe ser de tal manera que ofrezca un panorama amplio de los incidentes de seguridad que han ocurrido y podría ocurrir dentro de la compañía, para incrementa la agudeza de percepción.

Para poder lograr el cambio del comportamiento, M. Alexander, (2002) indica que con un programa de reforzamiento continuo sería mucho más fácil.

El reforzamiento continuo puede llevarse a cabo mediante Trainings, publicaciones, seminarios, y otra clase de intervenciones enfocadas a los riesgos en la organización, para los cuales debemos de calcular la frecuencia en la que se deben de aplicar. Esta frecuencia se definirá en la variable "Número mínimo de sesiones de reforzamiento instrumental al año".

Para calcular el valor de la variable "Número mínimo de sesiones de reforzamiento instrumental al año", haremos lo siguiente.

En la figura 4, tomada del modelo original, se representa el efecto que ejerce la percepción del riesgo sobre la conformidad. En ella podemos apreciar que la extinción de la "conformidad" toma aproximadamente un año.

El lapso de tiempo que toma en desvanecerse la conformidad, desde su punto máximo hasta el punto en que se cruza con el límite de la zona de riesgo, es de aproximadamente 2 meses. Este es el tiempo que tarda en presentarse la extinción de la conformidad, implicando una disminución en la respuesta instrumental *(aumento de la percepción del riesgo y la conformidad).*

El tiempo total que toma en extinguirse por completo la conformidad, dividido entre el tiempo en que tarda en presentarse su extinción. 12meses/2meses = 6; lo cual indica que al

año se deben de ejecutar seis sesiones de reforzamiento para mantener los niveles de seguridad.

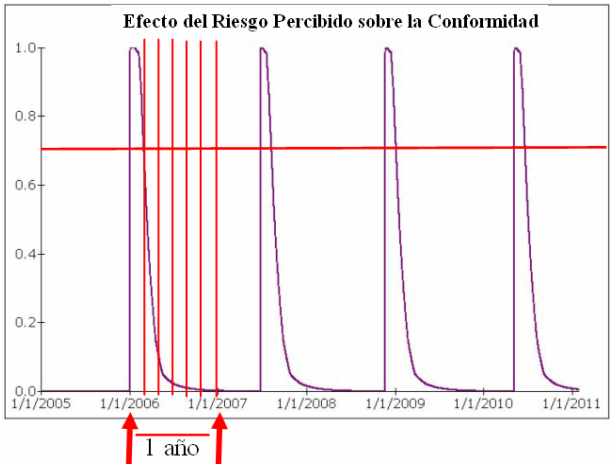


Figura 5.- Tiempo de decremento del nivel de conformidad. Gráfica tomada de González, (2002).

Para la variable "Sesiones de Reforzamiento Instrumental programados al año", el valor que puede tomar debe ser igual o mayor que el valor definido para la variable "Número mínimo de Sesiones de Reforzamiento Instrumental al año"; de manera contraria, el reforzamiento instrumental no tendrá efecto.

El BBP, la percepción de riesgo y conformidad, se han programado para un crecimiento diario durante un período de 15 años, si el reforzamiento instrumental esta presente.

Estos crecimientos se representan con las siguientes tasas de incrementos:

El BBP parte de un valor inicial por defecto, el cual es (1/14 de tsk/da), al final de los diez años de simulación, se pretende tener un incremento total de 3/14 de tsk/da. lo que nos da un margen para incrementar del 2/14 de tsk/da. Este es el valor de la variable "Tasa de incremento del BBP".

- Tasa de incremento del BBP = = 0.00003968253968254 tsk/da²

El "tiempo de disminución de la percepción de riesgo" comienza con un valor de 10 semanas, al cual el programamos un aumento de 4 semanas, al final de los 10 años, tendrá un valor de 60.

- Tasa de incremento de percepción = 0.02722222222222

El “tiempo de extinción de la conformidad” comienza con un valor de 50 semanas, al cual le programamos un aumento de 20 semanas al termino de los 10 años, su valor será de 70 semanas.

- Tasa de incremento de la Conformidad = 0.03888888888889

Estos valores que han sido tomados para las tasas de incrementos, han sido únicamente con el propósito de simular un incremento en estas variables, ya que no existe un valor de incremento establecido; Se tendrían que hacer estudios referentes a estos incrementos en el comportamiento humano.

4.4.- Método

Conociendo las variables que intervienen en la seguridad en una organización, se necesitará integrarlas en una visión conjunta, que nos permita configurar la seguridad de nuestra organización mediante un proceso definido y aplicable.

Un Modelo de Seguridad de la Información, basado en la Dinámica de Sistemas que represente el conjunto de variables interactuando es la opción más eficaz para implementar los modelos y políticas adecuadas a la organización y a poder visualizar las propiedades funcionales y estructurales de la seguridad de nuestro sistema.

El modelo que empleamos esta pensado para empresas las cuales cumplan con ciertas características de seguridad. Estas características nos darán las posibles situaciones y vulnerabilidades que se pudieran presentarse en las compañías en lo que a la Confidencialidad, Integridad y Disponibilidad de sus servicios e información se refiere.

- Cuente con un departamento encargado de los Sistemas de Información.

- Que cuenten con procedimientos establecidos para el manejo de la información y los servicios (políticas).

- El personal a cargo de los sistemas de información tenga conocimiento de lo que son las amenazas a la información.

4.4.1.- La metodología a seguir

- Análisis de variables: En esta primera etapa se estudia el modelo propuesto por González, (2002); para entender las variables y su comportamiento.

- Calibración del modelo: Se generarán las primeras pruebas del modelo con el software de simulación (en este caso el Powersim) con el propósito de observar

y confirmar que se están obteniendo los mismos resultados que en el trabajo de González, (2002).

- Dinámica general del modelo: Una vez contando con los datos y variables, se estudiarán sus ecuaciones e interacciones dinámicas que tienen cada una de ellas entre sí para poder entender la dinámica general.

- Tabla de variables: Se creará una tabla de todas las variables que intervienen en el modelo causal en la que se explicará de manera clara cada una de las ellas.

- Investigación de métodos para influir en los patrones de comportamiento humano aplicando el condicionamiento instrumental. Estos comportamientos son la "percepción del riesgo", la "conformidad" con los niveles de seguridad, la "distribución preferida de actividades de seguridad" (BBP).

- Aportación al modelo: integración al modelo de las variables del condicionamiento instrumental que modificarán el comportamiento original del sistema.

- Simulaciones: Se realizarán simulaciones y se estudiará el comportamiento del sistema.

- Comparaciones: Los resultados de las simulaciones, después de aplicado el condicionamiento instrumental, serán comparados contra las simulaciones originales.

- Resultados obtenidos de las simulaciones.

Capítulo 5: Resultados

5.1.- Síntesis

En este capítulo veremos los resultados obtenidos en las simulaciones, los cuales se han dividido en dos grupos.

En los tres grupos, se describe el comportamiento del modelo partiendo de una percepción de riesgo elevada, debido a la acción de condicionamiento de un incidente inicial, la cual, al paso del tiempo, se va desvaneciendo. Se aprecia como entran en juego las variables siguientes: Distribución preferida de actividades de seguridad (BBP), Riesgo Percibido, Conformidad, Nivel de seguridad y los incidentes de seguridad, creando un ciclo en el que se repite el proceso durante el tiempo establecido de simulación.

En el grupo de simulación 1, se tienen incrementos en los valores de las variables en un solo salto. Esto es: al instante en el que se presenta el condicionamiento instrumental las variables pasan de un valor V1 $\Rightarrow$V2.

En el grupo de simulación 2, los incrementos de las variables se hacen a través de tasas de incremento diarias. Esto es: al instante en el que se presenta el condicionamiento instrumental, las variables empiezan a incrementarse gradualmente mediante la tasa de incremento diario.

En el grupo de simulación 3, los incrementos de las variables se hacen, de la misma manera que en el grupo de simulación 2. La diferencia radica en que la variable distribución preferida de actividades de seguridad (BBP), no cambia de su valor inicial = 1/14 tsk/da, permaneciendo constante.

5.2.- Resultados

5.2.1.- Grupo de prueba 1

5.2.1.1.- Escenario

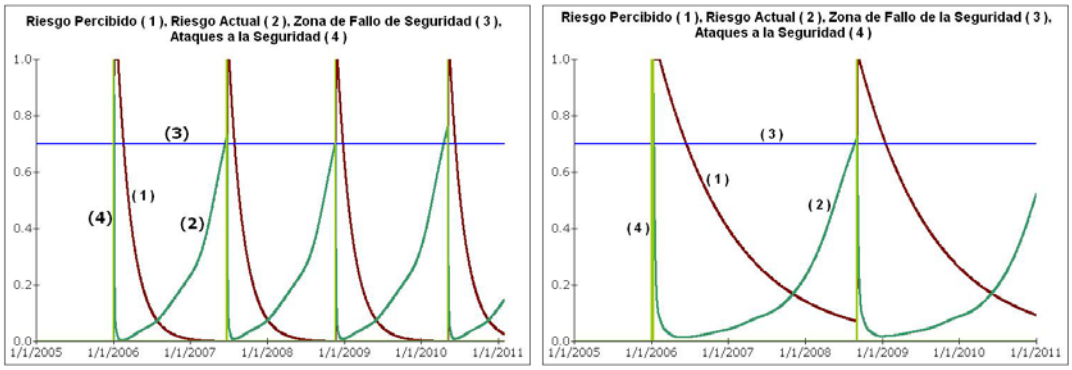
En el grupo de pruebas 1 se presentan las interacciones de las variables Riesgo Percibido, Conformidad, Nivel de Seguridad y el BBP; los cuales interactúan partiendo de de la siguiente premisa: al presentarse el primer ataque a la seguridad, la percepción de riesgo se incrementa al máximo, modulando la conformidad y esta a su vez el nivel de seguridad. sobre estos niveles de percepción, conformidad y seguridad, aplicamos el reforzamiento instrumental.

Lo que este reforzamiento hace matemáticamente, es afectar las variables que se encuentran en el modelo a bloques (modelo que contiene las ecuaciones matemáticas que corre el programa de simulación); las cuales indican el tiempo en el que la conformidad se extingue "extinction time" y la disminución de la percepción de riesgo "risk perception attrition time", ésta variables tienen los siguientes valores:

"Extinction Time" inicia con un valor de 50 <<wk>> el cual cambia a 70<<wk>>. "Risk perception attrition time" inicia con un valor de 10 <<wk>>, el cambia a 50<<wk>>. El BBP inicia con un valor de 1/14 tsk/da y cambia a 3/14 tsk/da. Estos aumentos se dan con la condición de que el Reforzamiento Instrumental esté presente.

5.2.1.2.- Simulación

Comparando las gráficas de simulación del modelo original contra las del modelo afectado con el condicionamiento instrumental, se obtuvieron los siguientes resultados:



a) (González, 2002) **b) simulación propia.**

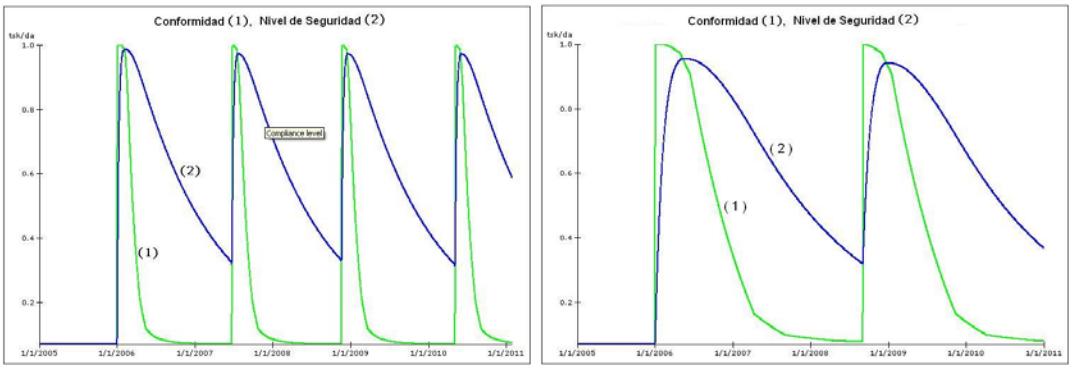
Gráfica 1.- Las gráficas a) y b) muestran el comportamiento del sistema con respecto al riesgo percibido, el riesgo actual y los ataques a la seguridad.

Un punto muy importante aquí tomado a manera de Set Point para el nivel de seguridad en la simulación, es LA ZONA DE FALLO DE SEGURIDAD. este Set Point, representado por la línea horizontal marcada con el número (3), indica el valor en el que el incremento del riesgo actual disparará los ataques a la seguridad en el sistema.

La PERCEPCIÓN DEL RIESGO indicada en la gráfica 1 a) y b) con la línea marcada con (1); se disminuía en un tiempo aproximado de 1 año en la (Gráfica 1a); ahora con el número la aplicación del condicionamiento instrumental (Gráfica 1b), se logró aumentar el tiempo que toma en disminuir. Se puede apreciar que la percepción del riesgo ya no toma valores de cero, lo cual, nos indica que siempre existe una alerta.

Los ATAQUES a la seguridad se desplazaron en tiempo, esto es, que de presentarse con una frecuencia de alrededor de 1.5 años, ahora se presentan con una frecuencia de 2.8 años, esto se puede apreciar en la Gráfica 1a y Gráfica 1b con la línea marcada con el número (4).

Esta disminución de la frecuencia de los ataques se explica por el incremento de la percepción del riesgo.



a) (González, 2002) **b) simulación propia.**

Gráfica 2.- Las gráficas a) y b) muestran la relación del incremento de la conformidad con respecto al nivel de seguridad.

La Gráfica 2a y Gráfica 2b, nos presentan el comportamiento de la CONFORMIDAD con la línea marcada con el número (1). En la Gráfica 2a, se puede apreciar como la conformidad disminuye en un lapso aproximado de un año, tiempo en el que alcanza su valor mínimo de cero.

En la Gráfica 2b, el comportamiento de la conformidad se modificó con el condicionamiento instrumental. Se aprecia, con la línea marcada con el número (1), un incremento en el tiempo de la conformidad. Este incremento es debido a que el riesgo percibido aumenta.

Este condicionamiento mantiene a los individuos alertas, incrementando y reforzando el conocimiento sobre los riesgos actuales, con lo que su nivel de conformidad, con las políticas de seguridad, perdura por más tiempo.

El NIVEL DE SEGURIDAD se aprecia en la Gráfica 2a y Gráfica 2b con la línea marcada con el número (2). El nivel de seguridad es modulado por la conformidad en un ciclo de retroalimentación positivo, y de acuerdo a esto, vemos que el nivel de seguridad aumenta o disminuye de acuerdo al comportamiento de la conformidad.

5.2.2.- Grupo de prueba 2

5.2.2.1.- Escenario

En este grupo de pruebas, los cambios primordiales, se dan alrededor de los incrementos que tienen las variables “BBP””, “extinction time” y “risk perception attrition time”. En este caso, los incrementos no se dan en un paso, sino que son incrementos por día, se va incrementando con forme a una tasa de incremento declarada para cada una de las variables.

- Tasa de incremento del BBP = = 0.00003968253968254 tsk/da
- Tasa de incremento de percepción = 0.02722222222222
- Tasa de incremento de la Conformidad = 0.03888888888889

Estas tasas son incrementos que se les van sumando a los valores iniciales de las variables mencionadas y están calculadas para que alcancen los siguientes valores en el transcurso de 10 años.

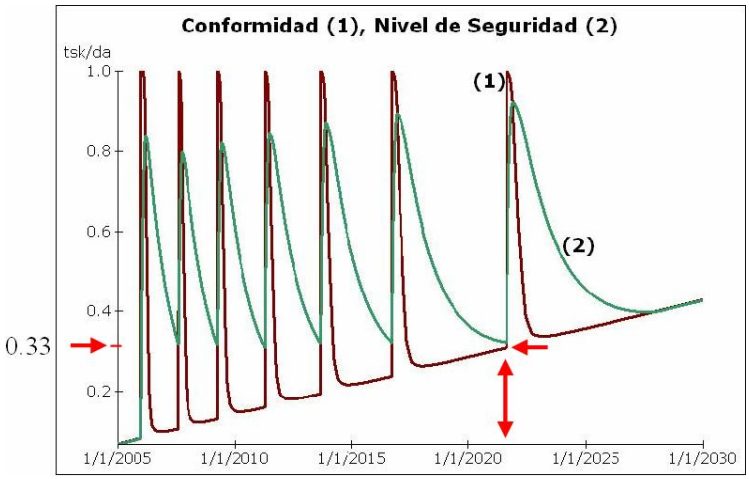
“Extinction Time” inicia con un valor de 50 <<wk>> el cual incrementa a 70<<wk>>. “Risk perception attrition time” inicia con un valor de 10 <<wk>> e incrementa a 50<<wk>>. El BBP inicia con un valor de 1/14 tsk/da e incrementa a 3/14 tsk/da.

Estos aumentos se dan con la condición de que el Reforzamiento Instrumental esté presente.

5.2.2.2.- Simulación

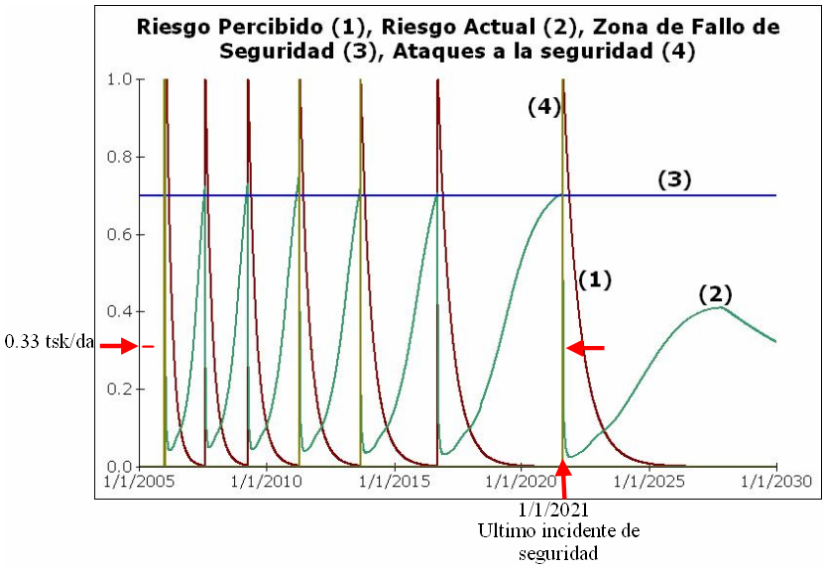
En la siguiente gráfica se muestran los comportamientos de la conformidad y los niveles de seguridad, la cual se va incrementando día a día, a través del condicionamiento instrumental.

Se puede apreciar como al ir incrementando la conformidad (línea marcada con el número 1), los niveles de seguridad (línea marcada con el número 2), se van manteniendo por más tiempo. Al ir subiendo la conformidad junto con los niveles de seguridad, llega un momento en el que la seguridad del sistema se encuentra en su máximo que ya no se presentan incidentes; esto lo apreciamos de la Gráfica 3, donde podemos observar que el ultimo incidente ocurrió antes de que la conformidad pasara el valor 0.33 tsk/da; aproximadamente en el año 2021 de simulación. Después de varias pruebas y simulaciones efectuadas, comprobamos que este valor de 0.33tsk/da es un umbral, cuando se adquieren valores arriba de este umbral, el sistema se vuelve totalmente seguro (cero incidentes).



Gráfica 3.- comportamiento de la conformidad y los niveles de seguridad. El aumento en tsk/da en el BBP se nota en el valor mínimo de la conformidad. Simulación propia.

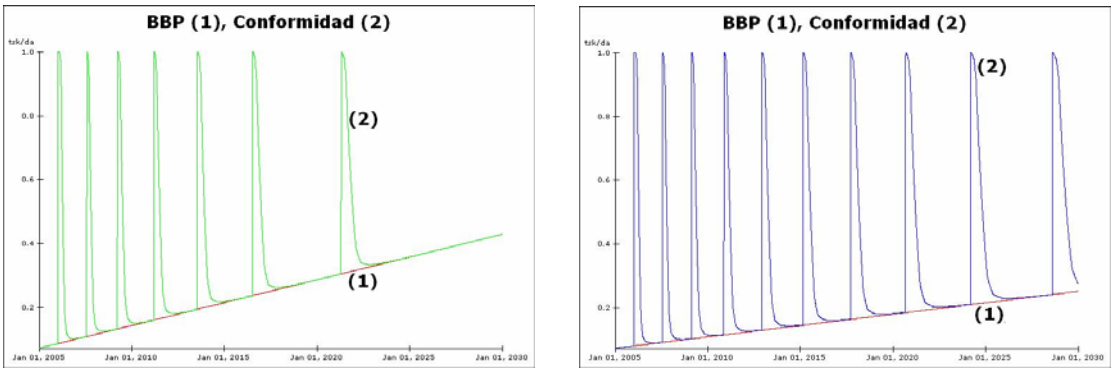
Gráfica 4, se aprecia los resultados que se tienen al irse incrementando la percepción de riesgo, los espaciamientos entre incidentes se va haciendo cada vez más largos; se aprecia que el ultimo incidente ocurre en la fecha indicada como (1/1/2021). El riesgo actual (línea marcada con el número 2) ya no vuelve a pasar la zona de fallo de seguridad (línea marcada con el número 3) después de esa fecha, esto hace que los incidentes ya no se presenten.



Gráfica 4.- En ésta gráfica se muestran la relación entre la percepción de riesgo y la frecuencia de incidentes. Simulación propia

De esto podemos apreciar que: los incidentes dependen de la percepción de riesgo y de la conformidad, ya que la percepción modula la conformidad y la conformidad indica los niveles de seguridad. Mientras la percepción de riesgo se va incrementando día a día, la conformidad igualmente se va incrementando

La conformidad es modulada por la percepción del riesgo. Al presentarse un incidente de seguridad, la percepción de riesgo se dispara hasta su máximo y así mismo, la conformidad se eleva para estar de acuerdo con los niveles de seguridad adecuados para mitigar el incidente. Una vez resuelto el problema los niveles de percepción de riesgo y conformidad disminuyen gradual mente, en un ciclo que inicia cada vez que se presenta un incidente.



a) BBP inicio 1/14 tsk/da ⇒final 3/14 tsk/da **b) BBP inicio 1/14 tsk/da ⇒final 2/14 tsk/da**

Gráfica 5.- Incremento de BBP a diferentes tasas a 10 años. Simulaciones propias

Al aplicar el reforzamiento instrumental, la percepción y la conformidad van aumentando de acuerdo a las tasas definidas para cada uno de ellos. Este aumento es en el tiempo que toma en disminuir la percepción y la conformidad, y en el caso del BBP, es un aumento del nivel de seguridad.

En la Gráfica 5a y Gráfica 5b, podemos ver como el aumento del BBP afecta a la conformidad, debido a que el mínimo valor permitido para la conformidad es el valor del BBP, el cual va aumentando con una tasa constante.

En la Gráfica 5a y Gráfica 5b, su hacen comparaciones de dos tasas de aumento. En la Gráfica 5a, tenemos una tasa de aumento del BBP mayor que en la Gráfica 5b. también se aprecia que los niveles de conformidad van aumentando conforme al incremento del BBP.

5.2.3.- Grupo de prueba 3

5.2.3.1.- Escenario

En este grupo de pruebas, los incrementos que tienen las variables, “extinction time” y “risk perception attrition time”, permanecen sin cambio.

- Tasa de incremento de percepción = 0.02722222222222
- Tasa de incremento de la Conformidad = 0.03888888888889

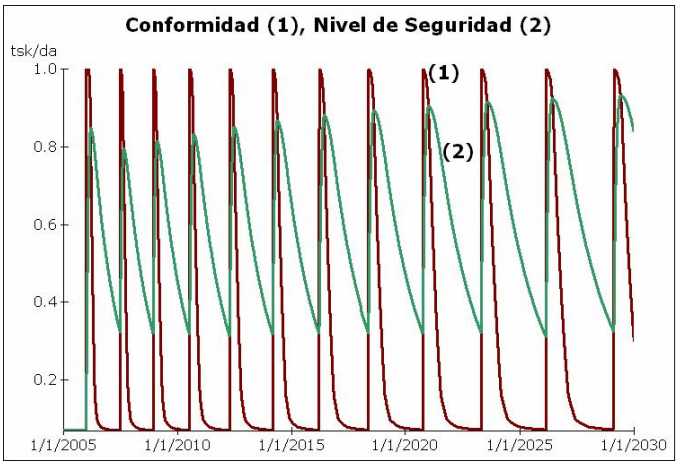
“Extinction Time” inicia con un valor de 50 <<wk>> el cual incrementa a 70<<wk>>. “Risk perception attrition time” inicia con un valor de 10 <<wk>> e incrementa a 50<<wk>>.

El cambio fundamental en esta simulación lo hacemos en el BBP, el cual no cambia y permanece constante con su valor de 1/14 tsk/da.

Esto es como indicio de que el aprendizaje en el BBP, a través de los reforzamientos instrumentales, no se haya dado.

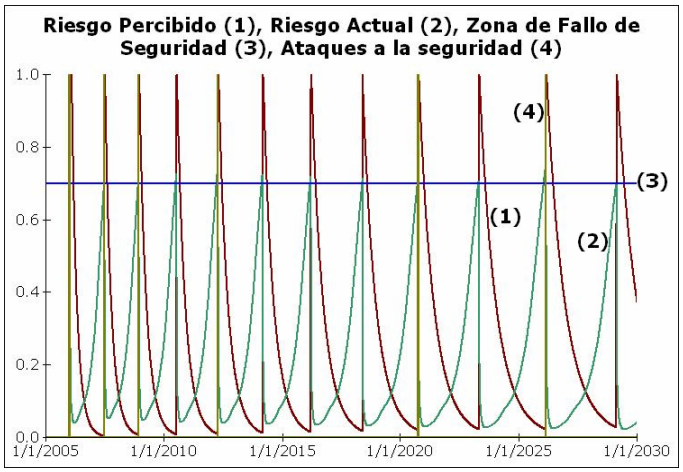
5.2.3.2.- Simulación

En la gráfica podemos observar como los incrementos en conformidad y el nivel de seguridad se van dando únicamente en el tiempo. En el grupo anterior, la conformidad iba incrementando el número de tareas por día (tsk/da) en las que estaba conforme.



Gráfica 6.- comportamiento de la conformidad y los niveles de seguridad, cuando el BBP no incrementa y se mantiene con su valor inicial constante. Simulación propia.

Los incidentes se van retardando cada vez más, esto es debido al aumento en los niveles de seguridad como respuesta al aumento diario de la conformidad y la percepción de riesgo.



Gráfica 7.- En ésta gráfica se muestran la relación entre el aumento de la percepción de riesgo y la disminución en la frecuencia de incidentes. Simulación propia

Dado que no existe un cambio en la distribución preferida de actividades de seguridad, el nivel mínimo que puede tomar la conformidad se mantiene siempre por debajo del valor umbral que hace al sistema completamente seguro (cero incidentes). Esta simulación la podemos llevar hasta valores de tiempo grandes de simulación y lo único que obtendríamos es un retardo en tiempo de los ataques, dado el aumento del tiempo de desvanecimiento de la percepción de riesgo y la conformidad con los niveles de seguridad.

Capítulo 2: Antecedentes

2.1.- Síntesis

La seguridad es un tema que ha tomado mayor interés en los últimos años y con la adquisición de nuevas tecnologías se han presentado nuevos problemas, para los cuales las empresas, independientemente de su tamaño; no estaban preparadas, Tao Peng et al (2003). La seguridad de la información es sin duda uno de los aspectos de mayor interés por la repercusión sobre las organizaciones, (King et al, 2003).

En este capítulo nos enfocaremos en la descripción de lo que la seguridad de la información es, como la ven las organizaciones, el crecimiento de las mismas y a los avances tecnológicos. Describiremos los riesgos a los que se ve sometida la seguridad de la información en una organización; hablaremos del factor humano y veremos por qué es considerado de mayor riesgo para la seguridad de la información dentro de una organización; se tratará la importancia de reconocer que los ataques internos son los más peligrosos, ya que, a diferencia del atacante externo; los empleados de una empresa poseen conocimiento y disponen de mayores oportunidades para explotar vulnerabilidades existentes, hablaremos de los efectos de los ataques a la seguridad de la información, y veremos que el cumplimiento de un ataque puede ocasionar desde pérdidas monetarias hasta pérdidas humanas, finalmente veremos los motivos más comunes por los cuales son atacadas las organizaciones.

La finalidad de este capítulo es el de proporcionar un punto de vista global a cerca de la seguridad de la información, poniendo las bases para poder entender la naturaleza de sus amenazas, motivos; y reconocer dónde se presentan la mayor cantidad de ataques y qué los provoca dentro de una organización.

2.2.-Seguridad

2.2.1.- La seguridad de la información

El manejo del flujo de la información nunca ha sido tan crítico o tan cambiante como en estos tiempos. A medida que los negocios crecen, los sistemas y la tecnología de información respaldan las operaciones de todas las comunidades de usuarios: clientes, proveedores, socios de negocios y empleados, por lo cual se requiere de un ambiente de control y seguridad para una gran variedad de información y transacciones, como por ejemplo: enviar ordenes, pagar cuentas, mantener los registros actualizados, etc. En consecuencia, existe hoy en día una creciente demanda para que las organizaciones

proporcionen el acceso adecuado tanto a las aplicaciones como a las instalaciones y en general, a los activos de información (PC News 1, 2004)

Tao Peng et al (2003) menciona que. “a consecuencia del 11 de septiembre” la gente se preocupo por la infraestructura de la seguridad de la información. La creciente inseguridad informática continúa su avance en todo el mundo de manera ascendente, lo que a hecho de la protección de la información una necesidad de todos: ya que la información es la base fundamental del funcionamiento de cualquier empresa, poniéndolas en riesgo al llegar a ser alcanzadas por cualquiera que logre penetrar su equipos e instalaciones y tener acceso a su información, pudiendo tomar, modificar o destruir todo lo que ahí se encuentre, poniéndolas en una muy grave situación.

Según la CERT/CC Overview, (2005); "La seguridad de la información es el proceso de prevenir y de detectar el uso desautorizado de los sistemas de información”. Las medidas preventivas le ayudan a detener a usuarios sin autorización (también conocidos como "intrusos") de tener acceso a cualquier parte de su sistema informático, la detección le ayuda a determinar si alguien intentó o no introducirse en un sistema, si tuvo éxito, y lo que pudieron haber hecho".

La seguridad de la información es sin duda uno de los aspectos de mayor interés por la repercusión sobre la empresa, por lo que se ha vuelto prioritaria la implementación de un programa de seguridad para protegerla, (King et al, 2003),

De acuerdo con King et al (2003), “el control de la seguridad de la información podría reducir el riesgo de exposiciones potenciales por individuos no autorizados a los recursos de la organización”.

Hoy en día, la protección de los activos de información y la seguridad informática ha pasado de ser un aspecto tecnológico basado en factores físicos, a constituir uno de los aspectos más importantes de las empresas, abarcando elementos de carácter lógico e incluso organizativos, (PC News 2, 2004)

Actualmente las distintas gerencias, han visto la necesidad de consagrar tiempo y recursos suficientes para que los activos de información estén suficientemente protegidos: “cuando ocurre un incidente grave que represente alguna debilidad en los sistemas informáticos, se deberán tomar las acciones correctivas rápidamente, para así reducir los riesgos”, (PC News 2, 2004).

El adquirir herramientas y metodologías, así como el constituir y desarrollar la Función de Seguridad de Activos de Información (FSAI), es una muestra clara de la madurez que ha ido alcanzado la conciencia de la alta gerencia en cuanto a que uno de los activos más importante de las empresas es la información y sus diferentes medios para generarla, almacenarla, transmitirla, e incluso; entregarla (PC News 2, 2004)

2.2.2.- Los Riesgos de la Seguridad de la información

De acuerdo a King et al (2003), las amenazas surgen en el entorno del sistema de información de la organización y pueden ser una persona, un software, un suceso, etc. que podría producir una violación a la seguridad del sistema de información, atentando con la confidencialidad, integridad y disponibilidad de ésta.

- **Confidencialidad:** Prevención del acceso no autorizado de la información.
- **Integridad:** Prevención de la modificación no autorizada de la información.
- **Disponibilidad:** Prevención de la retención no autorizada de la información o de los recursos.

Un ataque es la realización de cualquier amenaza, como podría ser:

- **Intrusión.-** alguien entra ilegalmente a un sistema y es capaz de utilizarlo y modificarlo como si fuera un usuario legítimo
- **Rechazo de Servicios.-** alguien logra que no puedan prestarse los servicios a los usuarios legítimos puede ser dañando al sistema o sobrecargado el sistema o la red
- **Robo de Información.-** alguien tiene acceso a información confidencial, secreta, reservada o restringida; es común en espionaje industrial, piratería, etc.

Las vulnerabilidades son representadas como la posibilidad que tiene el sistema de información de sufrir un ataque.

Como comenta D. Gollmann, (1999), "Uno de los primeros intentos que captura la noción de la seguridad de la información, es examinar como la información puede ser comprometida"

Novo y Urrutia, (2002); comentan que los ataques y amenazas pueden venir de diferentes individuos u organizaciones con diferentes técnicas y motivaciones, causando diversos efectos.

2.3.- El Factor Humano

"EL TALÓN DE AQUILES DE LA SEGURIDAD DE LA INFORMACIÓN"

Según Caruana, (2002); el factor humano es una parte esencial del juego de seguridad. No existe un sistema informático que no dependa de algún dato ingresado por algún

operador humano. Esto significa que esta debilidad de seguridad es universal, independiente de la plataforma, el software, red o edad de equipo que se trate.

Reason, (1997) citado por González, (2002); comenta que el factor humano está implicado en un 80% a un 90% en los accidentes organizacionales. González, (2002); dijo "El factor humano es el Talón de Aquiles de la seguridad de la información".

Caruana, (2002); ve a cualquier persona que tenga acceso a la organización o al sistema de información, ya sea física o electrónicamente, como un riesgo potencial de inseguridad

Uno de los principales errores es pensar que al contar con la tecnología de punta para la protección de la información y que controlen los accesos a los servicios de la empresa, se esta totalmente protegido, Schneier, (2000), en su libro "Secrets and lies: Digital Security in a Networked World", dijo: "Si piensas que la tecnología puede resolver tus problemas de seguridad, entonces no entiendes los problemas y no entiendes la tecnología".

2.4.- Los Ataques internos

M. Sisk, (2005); mencionó para una revista llamada Bank Technology News, una frase que suena a película de terror, "*el enemigo está adentro*".

En un principio las empresas consideraban que tenían que protegerse de los agentes y ataques externos, como aquellos que son derivados por el uso de Internet; pero con el paso del tiempo, las empresas han advertido que no sólo existen este tipo de amenazas, sino que también hay peligros dentro de la organización, y que éstos deberían ser contemplados a la hora de proteger la información, (PC News 4, 2004).

M. Sisk (2005) indica que las evidencias en problemas de seguridad de la información, están demostrando que las amenazas externas, son solo una porción y quizás no la porción mayor de las amenazas a la seguridad de la información más preciada por las organizaciones.

Según M Sisk (2005) una encuesta reciente del instituto de Ponemon de compañías financieras y no financieras, reveló recientemente que el 69 por ciento reportó serias fugas de datos debido a los errores malintencionados o no malintencionados de los empleados: 39 por ciento implicaron la información confidencial del negocio, 27 por ciento implicó información personal sobre clientes, 14 por ciento implicó propiedad intelectual, incluyendo códigos fuente de software y el 10 por ciento incluyendo información personal sobre empleados.

M Sisk (2005) indica que las brechas de la seguridad ocurren a menudo por la sencilla razón que de que los empleados no tienen conocimiento alguno de lo que es la seguridad de la información, está intentando hacer su trabajo rápidamente, o está intentando satisfacer a un cliente o a un socio.

Según Microsoft, (2002); los riesgos potenciales asociados con un ataque interno son mucho más altos hoy de lo que eran hace sólo dos años. Un ataque exitoso de negación de servicio puede realmente detener a toda una compañía, por eso es importante tener el conocimiento de que los ataques internos representan una amenaza importante para las empresas, por ser éstos causantes de daños patrimoniales significativos.

A diferencia del atacante externo, los empleados de una empresa poseen conocimiento y disponen de mayores oportunidades para explotar vulnerabilidades existentes. Por esta razón, los ataques internos siguen siendo altamente costosos y difíciles de identificar, (PC News 4, 2004).

2.5.- Posibles efectos de un ataque a la información.

Las amenazas a la seguridad que afrontan las empresas hoy en día tienen realmente la capacidad de acabar con una empresa, (Microsoft, 2002).

Según King ed al, (2003), el cumplimiento de un ataque puede ocasionar desde pérdidas monetarias hasta pérdidas humanas. "Típicamente una Organización incurre en dos tipos de pérdidas dadas estas amenazas: Pérdida Directa o Pérdida Consecuencial.

• Negación de servicio
• Uso no autorizado de los sistemas informáticos
• Pérdida/alteración/comprometer los datos.
• Pérdida monetaria/financiera.
• Pérdida o puesta en peligro vidas humanas.
• Pérdida de confianza en las redes de computadoras.
• Pérdida de confianza pública.

Tabla 1.- Efectos de los ataques.

La pérdida directa es cuando un sistema o componentes relativos a este sistema son dañados o destruidos.

La pérdida consecuencial podría ocurrir como resultado de la pérdida directa y puede ocurrir en muchas formas como: pérdidas de clientes, pérdida de Proveedores, vergüenza pública, pérdidas en las ventajas competitivas e información, pérdidas tangibles de activos y decrementos del flujo de efectivo, pudiendo llegar también a exponer o perder vidas humanas.

¿Quienes atacan al sistema de información?

• Intrusos Adolescentes
• Espías Industriales
• Trabajadores Internos
• Gobiernos Foráneos
• Criminales

Tabla 2.- Agentes agresores de la Información.

2.6.- Motivos para atacar los sistemas de información.

Según comenta Novo y Urrutia (2002), Los motivos para decidir atacar una organización pueden variar caso por caso. Existen muchos individuos u organizaciones que intentan infiltrarse a una organización, con múltiples intereses, ya sea financieros, políticos o simplemente vandalismo.

De acuerdo a C.King (2003), los motivos por los cuales un intruso decide entrar a un sistema son muy diversos, algunos ejemplos podrían ser: robo de información valiosa, diversión, desafío personal, curiosidad, venganza etc.

Dinero, lucro.
Acceso a recursos adicionales.
Ventaja competitiva - Económica - Política
Protesta, venganza
Curiosidad
Desafío personal
Llamar la atención

Tabla 3.- Motivos de ataques..

Según CERT/CC, (2003), usualmente no es posible determinar el motivo por el cual se esta bajo ataque.

Capítulo 6: Conclusiones

6.1.- Conclusiones

Como producto de las simulaciones realizadas y de los resultados obtenidos que fueron mostrados en el capítulo anterior, se han planteado las siguientes conclusiones.

6.1.1.- De las simulaciones

De acuerdo a las simulaciones realizadas, se puede observar que un factor muy importante para lograr mejores resultados en la seguridad son los incrementos de la distribución preferida de actividades de seguridad (BBP), los cuales resultan de la aplicación del condicionamiento instrumental. Esto se vio en los grupos de simulación 1 y 2.

Es importante notar que el BBP solamente puede aumentar, pasando de una distribución de actividades $BBP_1 \Rightarrow BBP_2$, donde $BBP_2 > BBP_1$. Esto es debido a que es un comportamiento que se define como "punto de confort" y lo mínimo que puede hacer una persona, con respecto a actividades de seguridad, está indicado en su BBP.

De acuerdo a las simulaciones hechas en los grupos de simulación 1 y 2, la conformidad va incrementando su valor mínimo conforme al incremento del BBP, esto nos indica que el BBP marca el valor mínimo de la conformidad, lo cual incrementa el nivel de seguridad.

De acuerdo al incremento que vaya sufriendo el BBP, puede llevar al sistema a un estado de cero incidentes. Este estado se alcanza cuando el BBP adquiere valores arriba de 0.33<<tsk/da>>.

Por otro lado, es importante mantener una satisfacción y motivación de los individuos dentro de la empresa; ya que la insatisfacción de las personas es un riesgo potencial que se debe tomar en consideración.

6.1.2.- De seguridad

Es usual que en las empresas en las que existen departamentos de seguridad; estos están subvalorados, distorsionados y normalmente son sometidos a decisiones de otros departamentos; como son vistos como servicios internos o externos independientes de las

funciones que aportan valor a la organización, no se les considera importantes o que en vez de portar beneficios a la empresa, solo estorban para ello.

La seguridad es mucho más que un servicio a la organización, es una función que está ligada a cada una de las otras funciones de la organización. Por ello se debe tener en claro que es la seguridad, para que sirve y como se gestiona, y de que manera esta pueda aportar beneficios a la organización.

Hay que entender que la seguridad corporativa no es solo la protección física de la empresa, sino que también aporta un beneficio a la empresa en términos económicos y financieros. Ya que a través de ella se pueden manejar datos e información secreta de la posición estratégica de la empresa, usuarios, clientes, información de productos, etc.

Ya que la información es el bien más importante para una organización, se debe de proteger en cada uno de los procesos y funciones de la empresa; la seguridad no puede verse como una función independientes de las demás. Por esto, es importante poder adaptar la seguridad a otras funciones corporativas en los tres niveles siguientes: estratégico, organizativo y de gestión.

A parte de asesorar en los proyectos, sistemas o guardia; se debe permitir que el ejecutivo de seguridad pueda asesorar en la política y estrategia de la organización.

6.2.- Trabajos futuros

Ya que son muchos los factores que intervienen en la seguridad en una organización y las ecuaciones que pueden describir los comportamientos e interrelaciones de casa una de ellas, y éste modelo de seguridad presentado, solamente muestra los principales factores, los cuales nos hacen una referencia de la realidad.

Se proponen como trabajos futuros de contribución al modelo:

- **Integrar nuevos factores** que hagan de las simulaciones un acercamiento más a la realidad en una organización.

- **Modificaciones a las ecuaciones de las variables.** Con esto se podría tener otra visión y nuevas formas de relaciones de las variables.

- **Realizar un modelo más específico,** que represente a un tipo de empresa en especial, con características propias y nuevas ecuaciones que definan su comportamiento.

- **Definir cambios en las relaciones de las variables** debido a introducción de políticas y normas de seguridad.

Apéndice A: Descripción de las Variables del modelo causal

VARIABLES DEL MODELO

- **.BBP (Behavioral Bliss Point):** Es la distribución preferida de las actividades de seguridad.

- **Efecto del Riesgo percibido en la Conformidad:** Esta variable representa la manera en como la conformidad con el nivel de tareas de seguridad va disminuyendo conforme el tiempo transcurre y la percepción del riesgo disminuye.

- **Nivel de Seguridad:** Esta variable es el indicador del nivel de seguridad que se tiene en un instante de tiempo

- **Nivel de Seguridad Preferido:** Esta variable esta muy influenciada por el BBP, el cual la regula. Cuando el nivel de conformidad cae al mínimo, el BBP es el que declara el nivel de seguridad preferido. Cuando el nivel de conformidad es alto, se toma el nivel apropiado de seguridad definido por las políticas de seguridad (nivel de seguridad prescrito)

- **Nivel de Seguridad Prescrito:** Esta variable esta directamente ligada a las políticas. En las y lo que se debe seguir con respecto a las amenazas externas e internas que se presentan en la organización.

- **Riesgo Actual:** Es el Riesgo que se presenta en un instante de tiempo.

- **Riesgo Interno y Externo:** Esta variable representa los riesgos que potenciales dentro y fuera de la organización..

- **Riesgo Percibido:** Esta variable se ve afectado en el tiempo por una percepción del riesgo actual dado que no ocurren ataques por un período de tiempo considerable.

- **Taza de Ajuste del Nivel de Seguridad:** Es la taza con la que se ajusta el nivel de seguridad y esta definida por el nivel de seguridad preferido.

VARIABLES DEL REFORZAMIENTO INSTRUMENTAL

- **Determinador del Reforzamiento instrumental:** esta variable evalúa si las intervenciones programadas al año son suficientes para poder mantener al individuo con una percepción de riesgo alta, incrementando y refrescando el conocimiento de los usuarios sobre los riesgos de las TI´s. En caso contrario la conformidad decrementará y el Behavioral Bliss Point actuará. Esta variable modifica el BBP incrementando su valor por sobre un valor inicial establecido por el usuario.

- **Numero mínimo de sesiones de reforzamiento instrumental al año:** Es la cantidad de intervenciones mínimas al año que se debe tener programado para incrementar y refrescar el conocimiento de los usuarios sobre los riesgos de las TI´s.

- **Sesiones de reforzamiento instrumental programados al año:** Es la cantidad de intervenciones enfocadas a los riesgos que se tienen programados realmente al año para el personal de toda la compañía, con el propósito de mantener informados y alertas de los sucesos e incidentes antes ocurridos en el transcurso del año. Trainings, publicaciones, seminarios, y otra clase de intervenciones enfocadas a los riesgos en TI, son buenas herramientas potenciales para incrementar y refrescar el conocimiento de los usuarios sobre los sistemas de TI´s, (González, 2002).

Apéndice B: Ecuaciones del modelo causal

	VARIABLE	ECUACION EN POWERSIM	DESCRIPCIÓN
1	After one Time Constant	EXP(-1)	Duración de accidentes
2	Behaivioral Bliss Point	1/14 tsk/da	El BBP es la distribucion preferida de las actividades de seguridad en ausencia de una restricción de procedimiento; en este caso se tiene que se realiza una actividad de seguridad cada 14 días dado que no hay nada que haga cambiar ese patron de comportamiento preferido.
3	Compliance Level	Behaivioral Bliss Point	Esta variable de nivel tiene como valor inicial el número relevamte de tareas de segurida por unidad de tiempo que esta dado por el BBP
4	Compliance Level Decay Switch	if(Prefered Compliance Level < Compliance Level,1,0)	Switch que dispara el decaimiento de la conformidad
5	Conditioning of Compliance	(1-Compliance level decay switch) * (Preferred compliance level-Compliance level)/Conditioning time	Tasa que describe el incremento de la conformidad como resultado de un cambio en la percepción del riesgo
6	Conditioning Time	1 wk	Es el tiempo promedio en el que el condicionamiento surge efecto
7	Current Risk	External Risk * Efect of compliance Level on Current Rick	Nivel de riesgo que caracteriza el entorno en un punto particular de tiempo. El nivel depende del nivel de Compliance: mientras el nivel de proteccion sea menos seguido, más aumenta el riesgo. So no se sigue ninguna medida de seguridad, el nivel de riesgo sera igual al nivel de riesgo externo.
8	Decrease of Risk Perception	(1-Security Failures)*(Percibed risk/Risk Perception Attrition Time)	Tasa en la que el sujeto se olvida del riesgo presente en el entorno. La precepción de que el riesgo decae toma lugar si no hay (o son pobres) noticias sobre fallas en la seguridad
9	Effect of Compliance Level on Current Risk	GRAPHCURVE(Compliance, 0 <<tak/da>>, 0.1<<tak/da>>, {1, 0.99, 0.97, 0.79, 0.4, 0.19, 0.11, 0.08, 0.05, 0.03, 0 //Min:0; Max:1//}	Mientras más alto sea el nivel de conformidad (se incrementa la seguridad), menor sera la expsosición al riesgo, esto es, que el nivel de riesgo disminuye
10	Effect of Perceived Risk on Compliance	GRAPHCURVE(Percived Risk, 0 <<rsk>>, 0.1<<rsk>>, {0, 0.01, 0.03, 0.1, 0.3, 0.5, 0.7, 0.9, 0.97, 0.99, 1 //Min:-0.1; Max:1.1//}	Mientras mas alto sea el riesgo que se perciba en el entorno, se mantendra una mayor actitud de conformidad y el individuo tendrá más ánimos de cumplir con la protección prescrita.
11	External Risk	IF(TIME<High Risk Start Date, 0<<rsk>>, 1<<rsk>>)	Nivel de riesgo (probabilidad de una mayor ataque por unidad de tiempo)
12	Extintion of Compliance	Compliance Level Decay Switch * (Compliance Level - Prefered Compliance Level)/Extintion Time	Tasa que describe el decaimiento del nivel de seguridad com resultado del retorno gradual hacia el Behaivioral Bliss Point.
13	Extintion Time	50 <<wk>>	Tiempo promedio que toma en extinguir el compliance (lo que permite que el nivel de seguridad decresca)
14	High Risk Start Date	STARTTIME + 1 <<YR>>	desde este d[ia el riesgo externo incrementa
15	Increase of Perception	'Security failures' * ('External risk'-'Perceived risk')/'Perception adjustment time'	Taza de incremento de la persepción de riesgo del sujeto: una actualización inmediata del nivel de conocimiento original es asumida en caso de noticias hacerca de fallas de seguridad.
16	Min Time Interval for Accidents	1 <<da>>	Used in conjunction with RANDOM to eliminate the effect of timestep (RANDOM generates one event per timestep, but we wish that only one stochastic event per 'Min time interval for accidents' counts). NOTE: This constant is not shown (is hidden=excluded) in the stock-and-flow diagram.
17	Perception Adjustment Time	1 // Security failures lead to quick adjustment of risk perception	Tiempo promedio que toma en incrementarse la persepción individual del riesgo. Una vez que las noticias de un fallo llegan, la percepción del riesgo es actualizada de inmediato. Pero aun si el impacto del fallo de seguridad es grande. Asumimos que lleva un tiempo medible en asimilar la mayor parte del incidente.
18	Percived Risk	External risk'	Es la percepción que tiene el sujeto del nivel de riesgo en el entorno.

Continuación

	VARIABLE	ECUACION EN POWERSIM	DESCRIPCIÓN
19	Preferred Compliance Level	Behavioral Bliss Point' + ('Prescribed compliance level' - 'Behavioral Bliss Point') * 'Effect of perceived risk on compliance'	Nivel de compliance actualmente preferido por el sujeto. Notece que la preferencia del sujeto es moldeada por la percepción de riesgo. Así, la percepción del riesgo actua como un instrumento de contingencia. Notece tambien que al BBP se asume que es cero riesgos percividos.
20	Prescibed Compliance Level	IF(TIME < 'High risk start date', 'Behavioral Bliss Point', 1 <<tsk/da>>)	Políticas de seguridad prescritas por la compañía
21	Pulse Height|	100	La altura del pulso usado para definir los incidentes de seguridad.
22	Risk Perception Attriction Time	10 <<wk>>	Tiempo promedio que toma a un individuo en olvidar hacerca de los riesgos presentes en el entorno.
23	Security Attacks	IF ('Current risk'<'Security failure zone',0,1) * PULSEIF(RANDOM(NUMBER('Security failure zone'),1)<=NUMBER('Current risk'),'Pulse height'*TIMESTEP) * IF(TIMECYCLE(STARTTIME, 'Min time interval for accidents', TIMESTEP),1,0)	Una vez que el riesgo actual entra en la zona de fallo, los ataques pueden ocurrir. PULSEIF(RANDOM(NUMBER('Security failure zone'),1)<=NUMBER('Current risk'),'Pulse height'*TIMESTEP) : un pulso ('Pulse height') es generado si un npumero aleatorio dentro del intervalo ['Security failure zone', 1] es menor que el 'Current risk'. Mientras 'Current risk' incrementa, la probabilidad de que dicho número aleatorio satisfaga la condición incrementa. El pulso puede ser utilizado para simular un fallo en la seguridad. De cualquier manera, desde que un número aleatorio es generado por RANDOM cada 'timestep'. De acuerdo al ultimo valor, IF(TIMECYCLE(STARTTIME, Min time interval for accidents, TIMESTEP),1,0) asegura que solamente un numero aleatorio sea tomado en cuenta cada 'Min time interval for accidents'.
24	Security Failure Impact Time	10 <<da>>	EL tiempo promedio que las fallas de seguridad hacen durar el impacto.
25	Security Failure Zone	0.7 <<rsk>>	Unbral pora el nivel de riesgo en el que los ataques pueden suceder.
26	Security Failures	IF(DELAYINF('Security attacks', 'Security failures impact time',1,0)*('Security failures impact time'/TIMESTEP)>='Pulse height'*'After one time constant', 1, 0)	Apreciasión individual del éxito de los ataques. El sujeto aprende de los ataques con un retardo. El tiempo de impacto de los fallos de seguridad indican que tanto los ataques exitosos impactan la percepción del riesgo. (si los fallos de suguridad = 1 la percepción del riesgoincrementa hacia 1<<rsk>>, lo que es el valor máximo valor de riesgo que se puede asumir en este modelo.
27	Security Level Gap	IF('Preferred compliance level' >= 'Compliance level','Preferred compliance level' - 'Compliance level', -('Preferred compliance level' - 'Compliance level'))	Degree to which the individual must change his behavior to follow the currently preferred security level. Note that the gap is always positive, no matter whether the set point is higher or lower than the current 'Security level'.

Estas ecuaciones son teóricas. Un intento por representar la realidad dentro de un modelo de seguridad simulado.

Las ecuaciones presentadas aquí, muestran un set de instrucciones, las cuales son propias del programa de simulación empleado. Por lo que en el documento no se muestran más que las relaciones y flujos entre variables.

Apéndice C: Ejemplo de aplicación del modelo de seguridad.

Supóngase una empresa en la que se mantiene un nivel de seguridad prescrito por las políticas de seguridad de la organización de la siguiente manera:

- **POLITICA:** Para el control de la entrada a personas ajenas a las instalaciones se debe de llenar una bitácora con los datos y nombre de la persona a la que viene a ver y asuntos a atender.

La persona a la que se le encarga el cuidado de la entrada lleva casi medio año trabajando en el mismo puesto y atiende una cantidad considerable de gente al día, que entra y sale de la empresa.

Durante más de 6 meses no se han presentado ni una clase de incidentes de seguridad dentro de la empresa. Esta persona encargada de la seguridad de la entrada a las instalaciones empieza a ver los niveles de seguridad con una inconformidad. Como su nivel de conformidad con ese nivel de seguridad ha empezado a decrecer, decide dejar pasar a la gente que conoce sin tenerse que registrar. Este hecho le permite al guardia ahorrarse trabajo y hacer el trabajo un poco más fácil.

Conforme continúa pasando el tiempo y no se ha presentado los incidentes, su conformidad llega a niveles más bajos, tanto que decide olvidarse de las políticas de seguridad y comienza a actuar conforme a su propio criterio. Decide apuntar en la bitácora solamente a determinadas personas para cumplir, dejando pasar la gran mayoría sin tomar registro de las actividades a realizar dentro de las instalaciones y a las personas con las que tratará dentro.

Dos meses después, se presenta un incidente de seguridad en la organización. El incidente involucra una laptop que se ha perdido y que contiene información confidencial de clientes y proveedores de la organización.

Inmediatamente al ocurrir el incidente de seguridad, el guardia cambia su percepción del riesgo actual. Su conformidad cambia, de realizar las actividades como él quería a tomar las indicaciones que le marcan las políticas.

El incidente ha aplicado un condicionamiento instrumental sobre la percepción de riesgo y la conformidad, y por consecuente, los niveles de esas variables incrementaron. Por lo tanto el nivel de seguridad en la organización se eleva al máximo.

Analizando las causas del incidente, se tiene que: no fue causado por fallas en la tecnología utilizada para el monitoreo y control de accesos a las instalaciones. Tampoco fue causada por agentes externos a la organización. El punto aquí es que, éste incidente

fue provocado por un miembro del mismo equipo de seguridad, ya sea de manera intencional o no intencional.

A través de las mejoras propuestas por el modelo de seguridad basado en la dinámica de sistemas. Podemos mejorar las políticas aplicadas la seguridad de la organización. En este caso, se puede incluir una parte en las políticas que se centre en ver esta clase de factores que influyen o causan la mayor cantidad de incidentes dentro de la organización.

Ya que sabemos que estos incidentes son causados por la disminución de la percepción del riesgo, una desmotivación y pérdida de la conformidad con los niveles de seguridad y el inevitable decremento en los niveles de seguridad. Aplicando de manera de reforzamiento al condicionamiento instrumental, podemos hacer que las personas aprendan de los riesgos vividos y se vuelvan más sensibles en la percepción del riesgo presente.

Apéndice D: Software para las simulaciones

El software utilizado para las simulaciones es el PowerSim, el cual se puede descargar de la página siguiente:

URL: http://www.powersim.com

Para bajar el software, es necesario entrar a la dirección anterior y seguir estos pasos.

1. darle un clic al link “download”

2. Una vez dentro de powersim downloads, se entra a la opción de “more” de Powersim Studio 2005 Express.

3. una vez dentro de download powersim studio 2005 express, darle un clic al link Download Powersim® Studio 2005 Express...

4. llenar con los datos pertinentes y correo electronico para el envío de la licencia para el software Powersim

5. señalar la casilla con la siguiente información “I am a faculty member or student at an accredited university, and I require Powersim solely for non-commercial applications”, y “Submit” los datos.

6. enseguida aparecerá la liga para descargar el software.

Este software, es una potente herramienta de simulación de modelos de dinámica de sistemas. Cuenta con set de instrucciones muy potentes para poder programar las ecuaciones que describen cada variable.

BIBLIOGRAFÍA

A. Waissbein, (2004). Core Labs. Reserch and Development. Modelos de Seguridad.

C. Arellano et al, (s/f). Modelo de Seguridad para Sistemas de Trabajo Colaborativo (Sec-CSCW)

CERT/CC Overview (2003). Insident and vulnerability trends. Carnegie Mellon University. http://www.cert.org (Accesada 10 de marzo, 2005)

E. Prim, (1998). Libro electrónico. Ciencias De La Tierra Y Del Medio Ambiente. http://www.esi.unav.es/asignaturas/ecologia/Hipertexto/01IntrCompl/111Model.htm. (Accesado el 10 de Octubre de 2005)

Gollmann, Dieter, (1999). "Computer Security" Book, John Wiley y Sons, Inc.

Gonzalez et al (2002). A Framework for Human Factors in Information Security. Proceedings of the 2002 WSEAS International Conference on Information Security (ICIS'02).

Grupo de Modelación Dinámica de Sistemas, (2002). ITESM. http://www.mty.itesm.mx/dae/de/grupos/modelacion/gds1.htm. (Accesado el 10 de octubre de 2005)

Instituto Tecnológico de Sonora, ITSON, (s.f.). Introducción a la Dinámica de Sistemas. http://www.itson.mx

Jay Forrester (1964). Modeling the dynamic processes of corporate growth. Proceedings if the IBM Scientific Computing Symposium on Simulation Model and Gaming.

Jay Forrester (1961), Industrial Dynamics, MIT Press, Cambridge, MA.

J. Boske, (2002). Microsoft Corporation. Modelos de seguridad y escenarios para SQL Server 2000 Windows CE Edition 2.0

King et al, “Security Architecture: Design, Deployment and Operations”. Osborne McGraw Hill. 2003

Lee et al (2003) “On the issues of IP Traceback for IPv6 and Mobile Ipv6” Eight IEEE International Symposium on Computers and Comunication (ISCC’03)

M. Alexander, (2002). Una explicación acerca del Entrenamiento del Clicker. http://www.clickersolutions.com/

M. Caruana (2002). Breves conceptos sobre la Ingeniería Social. http://www.rompecadenas.com.ar/ingsocial.htm (Accesada 6 de marzo, 2005)

M. Sisk. Bank Technology News. Periodical. New York: Mar 1, 2005.Vol. 18, Iss. 3; pg. 38

Microsoft Corporation, (2002). Seguridad en el escritorio Microsoft: Documento técnico.

PC NEWS 1, (2004).- Identity Management, cuando la información es su más preciado activo. http://www.pc-news.com/detalle.asp?ida=1744&sid=&id=11
(accesado el 6 de marzo, 2005)

PC NEWS 2, (2004).- Prácticas de Seguridad de Activos de Información de las empresas en Venezuela. http://www.pc-news.com/detalle.asp?ida=1638&sid=&id=11 (accesado el 6 de marzo, 2005)

PC News 4, (2004).- Prácticas de Seguridad de Activos de Información de las empresas en Venezuela II. http://pc-news.com/detalle.asp?ida=1646&sid=&id=11. (Accesada 6 de marzo, 2005)

Políticas y Modelos de seguridad, (s.f.).
http://www.sc.ehu.es/jiwibmaj/ApuntesCastellano/TEMA_12-politicas-.pdf
(Accesado el 25 de marzo, 2005)

R Novo y C. Urrutia, (2002). "Proporcionando Seguridad a las Redes de Telecomunicaciones". http://www. sans.org/rr/

Schneier, B. (2000). Secrets and Lies: Digital Security in a Networket Word. New York, John Wiley and Sons, Inc.

Senge (1990); "La Quinta Disciplina: El arte y la práctica de la organización abierta al aprendizaje"; Granica / Vergara.

Swiss Re, (1998). Swiss Reinsurance Company. Safety culture – a reflection of risk awareness

T. Peng ed al. "Detecting Reflector Attacks by Sharing Beliefs" Globecom 2003

Universidad Carlos III de Madrid, (s.f.). Condicionamiento Instrumental. Interpretaciones Asociacionistas. http://www.uc3m.es/marketing2/interpretacionasoc.htm

V. Anderson et al, (1997). Systems Thinking Basics: From Concepts to Causal Loops. To the reader. Ed. Pegasus Communications.

Vennix et al (1996). Group Model Building: facilitating team learning using system dynamics, New York: John Wiley