EL ROL Y CONTRIBUCIÓN DE LOS SISTEMAS EXPERTOS EN LA PREVENCIÓN DE VULNERABILIDADES Y RIESGOS EN LAS REDES Y ESTACIONES DE TRABAJO

Por

Norman E. Cruz
Catedrático Auxiliar
Recinto Metropolitano
Universidad Interamericana de Puerto Rico

RESUMEN

Se conoce la enorme influencia que han alcanzado los sistemas de información en la vida diaria de las personas y organizaciones, y la importancia que tiene su progreso para el desarrollo de un país. Las transacciones comerciales, la comunicación, los procesos industriales, las investigaciones, la seguridad, entre otros son todos aspectos que dependen cada día más de un adecuado desarrollo de la tecnología informática.
Junto al avance de la tecnología informática y su influencia en casi todas las áreas de la vida social; ha surgido una serie de comportamientos ilícitos denominados, delitos informáticos. La tecnología electrónica está ganando cada día más adeptos a su utilización debido a los beneficios que presenta poder operar desde su hogar u oficina, ganar tiempo al no tener que hacer filas, y obtener la información requerida en el momento que se desea. Todos estos beneficios pueden verse perjudicados si no se adopta una correcta protección de la información en cuanto a los delitos informáticos.
Este estudio exploratorio procuró determinar si existe alguna forma de identificar y prevenir las vulnerabilidades y riesgos en los sistemas de información de las organizaciones y, si los sistemas expertos son una solución viable a la eliminación de dichos peligros.

INTRODUCCIÓN

Los objetivos principales de este estudio exploratorio fueron establecer: si existe alguna forma de identificar y prevenir las vulnerabilidades y riesgos en los sistemas de información de las organizaciones y, si los sistemas expertos son una solución viable a la eliminación de dichos peligros. Se desarrolló este estudio considerando la fragilidad que suponen los sistemas informáticos en empresas; tales como las instituciones bancarias.

La presente investigación se trazó como meta determinar si, en efecto, los sistemas de información pueden evitar ser blanco de intromisiones no autorizadas. Además, determinar si los sistemas expertos como herramienta avanzada dentro del campo de los sistemas informáticos pueden ayudar a desarrollar programados con niveles de seguridad fiables.

La seguridad de la información y del control de los procesos es una parte integral de las empresas. En la medida en que los procesos están más automatizados y existe una mayor integración de los sistemas de información y las redes corporativas, la seguridad de la información es aún más importante. La tendencia es incrementar la integración y conectividad de los sistemas, utilizar sistemas operativos y arquitecturas abiertas, protocolos de comunicación estandarizados y soluciones programadas de forma modular (Puyosa Piña, s.f.).

Antecedentes de la Investigación

El internet ha facilitado y promovido el desarrollo de las comunicaciones a nivel global en los últimos años. Este aumento en la comunicación, ha estado fuertemente ligado al desarrollo de nuevas redes y nuevas aplicaciones que permiten compartir más información entre usuarios remotos.

Ha surgido en las empresas, la importante función de los administradores de redes, los cuales deben entablar un uso correcto de la red y; a su vez, garantizar la seguridad y confidencialidad de la información que manejan. Sin embargo, cada día aumentan los ataques contra redes y contra computadoras conectadas a éstas. El nivel de sofisticación de estos ataques es cada vez mayor, lo cual exige el desarrollo y actualización de herramientas pertinentes (Acosta et al., 2004).

Por tanto, se puede evidenciar, la gran importancia de desarrollar mecanismos de

autoprotección contra estos ataques, los cuales deben pasar por una fase de identificación de los potenciales riesgos a los que se está expuesto, luego a una fase de análisis de las debilidades para posteriormente definir acciones de mejora y defensa así como planes de mitigación ante sucesos indeseables.

Planteamiento del Problema

Las investigaciones recientes han reconocido que los factores tecnológicos no son la única clave para la eficacia de los controles de seguridad informática, también hay una necesidad de comprender el impacto de los factores humanos y organizacionales (Beznosov y Beznosova, 2007; Botta et al., 2007). Si bien se han realizado estudios de los retos específicos de la gerencia de la seguridad informática (Audestad, 2005; Knapp et al., 2006; Koskosas y Paul, 2004) o conjuntos de desafíos a lo largo de uno de los factores (Chang y Ho, 2006; Kankanhalli et al., 2003), ninguno han proporcionado una visión global integrada de los retos que enfrentan los profesionales de la seguridad. Una mejor comprensión de cómo los diferentes elementos humanos, organizacionales y tecnológicos podrían explicar los diferentes factores que conducen a las fuentes de violaciones de la seguridad y vulnerabilidades en las organizaciones (Kraemer y Carayon, 2007). Por tanto, ¿son los sistemas expertos la opción para lograr desarrollar sistemas de información, lo suficientemente robustos, para advertir sobre posibles fallas de seguridad en las redes y computadoras de las empresas?

Justificación del Estudio

Durante el proceso de identificación y análisis del problema, no se encontró en la literatura—ni inclusive al buscar a través de bancos de artículos de asociaciones profesionales y académicas— trabajos que intenten establecer si es posible la identificación y prevención de vulnerabilidades y riesgos en los sistemas de información

de las corporaciones y, que simultáneamente, busquen determinar si los sistemas expertos son una posible solución a la eliminación de dichas exposiciones.

Tal vez, en estos momentos, no hay mayor preocupación en el campo de la tecnología de información que los ataques maliciosos a las redes y computadoras de las organizaciones (Diario Digital Aeronoticias, 2009). Este estudio puede ser punta de lanza para apoyar o no el argumento de que si las vulnerabilidades y riesgos son prevenibles, teniendo una combinación adecuada de seguridad informática, recurso humano y estructura organizacional. Además, de considerar si los sistemas expertos pueden ser explotados como herramienta para la erradicación de éstos, sin importar las artimañas que individuos puedan intentar para hallar fallas de seguridad en los sistemas informáticos.

MARCO CONCEPTUAL Ó TEÓRICO

La representación del conocimiento es una cuestión que se plantea tanto en la ciencia cognitiva como en la inteligencia artificial (Russell y Norvig, 2003). La ciencia cognitiva tiene que ver con cómo la gente almacena y procesa información (Luger, 1994). Mientras, en la inteligencia artificial, el objetivo principal es almacenar conocimientos para que los programas o aplicaciones de computadoras puedan procesar dicha información y lograr la similitud de la inteligencia humana (Nilsson, 1998; Russell y Norvig, 2003). En la inteligencia artificial, los investigadores han tomado la representación de las teorías de la ciencia cognitiva. Así, hay técnicas de representación, como normas y redes semánticas, que tienen su origen en las teorías del procesamiento de información humano. Dado que el conocimiento se utiliza para lograr un comportamiento inteligente, el objetivo fundamental de la representación del conocimiento es representar el conocimiento de una manera que se facilite la inferencia; es decir, sacar conclusiones a partir del conocimiento.

El término “cognitiva” en la ciencia cognitiva es utilizado para cualquier tipo de operación mental o estructura que puede ser estudiada en términos precisos (Lakoff y Johnson, 1999). Esta conceptualización es muy amplia, y no debe confundirse con la forma cognitiva que se utiliza en algunas tradiciones de la filosofía analítica, donde cognitiva tiene que ver solo con las reglas formales y condiciones semánticas verdaderas (Glock, 2008). La ciencia cognitiva es un campo grande, y cubre una amplia gama de temas sobre la cognición. Sin embargo, hay que reconocer que la ciencia cognitiva no está igualmente preocupada por todos los temas que podrían influir en la naturaleza y el funcionamiento de la mente o inteligencia. Los factores sociales y culturales, la emoción, la conciencia, los métodos comparativos y evolutivos suelen ser minimizadas o excluir de inmediato, a menudo en los principales conflictos filosóficos. Sin embargo, algunos dentro de la comunidad de la ciencia cognitiva consideran estos temas vitales, y promover la importancia de su investigación. Las preguntas esenciales de la ciencia cognitiva son: ¿Qué es la inteligencia?, y ¿Cómo es posible modelarla a través de los sistemas de computadoras?

La ciencia cognitiva se suele definir como el estudio científico de la mente o bien de la inteligencia (Luger, 1994). Prácticamente cada presentación formal a la ciencia cognitiva hace hincapié en que es un área de investigación altamente interdisciplinaria en la que la psicología, la neurociencia, la lingüística, filosofía, ciencias de la computación, la antropología y la biología son sus principales ramas especializadas o aplicadas. Por tanto, podrá distinguir los estudios cognitivos del cerebro humano, la mente y la inteligencia.

Por otra parte, la inteligencia artificial implica el estudio de los fenómenos cognitivos en las máquinas (Goebel, Poole y Mackworth, 1997). Uno de los objetivos

prácticos de la inteligencia artificial es implantar los aspectos de la inteligencia humana en las computadoras. Éstas también se utilizan ampliamente como una herramienta para estudiar los fenómenos cognitivos, mediante simulaciones para estudiar cómo la inteligencia humana puede ser estructurada (Strogatz, 2007).

Los modelos de computadora requieren una representación matemática y lógica formal de un problema. Los modelos de computadora son utilizados en la simulación y verificación experimental de diferentes propiedades específicas y generales de la inteligencia. Éstos pueden ayudarnos a comprender la organización funcional de un fenómeno cognitivo particular. Hay dos enfoques básicos para el modelado cognitivo. El primero se centra en las funciones mentales abstractas de una mente inteligente y que funciona con símbolos; y el segundo, que sigue a las propiedades neuronales y asociativas del cerebro humano, y se llama sub simbólico.

Los modelos simbólicos evolucionaron a partir de paradigmas de la informática con las tecnologías de los sistemas basados en el conocimiento, así como una perspectiva filosófica (Haugeland, 1985). Ellos son desarrollados por los investigadores cognitivos primero y más tarde fueron utilizados en ingeniería de la información para los sistemas expertos (Finkelstein, 1989, Giarratano y Riley, 2005). Desde principios de 1990, se fue generalizando sistemáticamente para la investigación de los modelos funcionales parecidos a la inteligencia humana y, en paralelo, desarrollado como un entorno simbólico de arquitectura cognitiva (Laird, Rosenbloom y Newell, 1987).

Mientras, que la sub modelización simbólica incluye modelos de redes neuronales (Marcus, 2001). Esa conexión se basa en la idea de que la mente o cerebro se compone de nodos simples y que la potencia del sistema proviene principalmente de la existencia y la forma de las conexiones entre los nodos simples. Según Dewdney (1997), algunos

críticos de este enfoque consideran que si bien estos modelos abordan la realidad biológica como una repetición de cómo funciona el sistema, carecen de maneras de explicar cómo son las conexiones de sistemas complicados. Aún con simples reglas son muy difíciles de explicar, ya que a menudo son menos descifrables que el sistema que modelan.

En todos los enfoques anteriores tienden a ser generalizados a la forma de los modelos computacionales integrados a una inteligencia abstracta o sintética, con el fin de ser aplicado a la explicación y al mejoramiento de la toma de decisiones individuales y organizacionales (Abraham, 1990; Kahneman y Tversky, 2000). Existe cierto debate en el campo en cuanto a si la mente es visto como un gran abanico de elementos pequeños pero débiles individualmente (es decir, las neuronas), o como una colección de estructuras de alto nivel tales como símbolos, esquemas y reglas. El primer punto de vista utiliza las conexiones para estudiar la mente, mientras que el segundo hace hincapié en cálculos simbólicos. Una forma de ver el asunto es si es posible simular de forma precisa un cerebro humano en un equipo sin precisión simulando las neuronas que componen el cerebro humano (Pinker y Mehler, 1988). Esto permitiría, en última instancia, tener la oportunidad de anticipar que puede hacer un individuo con un comportamiento inmoral al detectar una falla de seguridad en los sistemas informáticos.

PREGUNTAS DE INVESTIGACIÓN

Con el rápido crecimiento del comercio electrónico, las agencias gubernamentales y las empresas están tomando precauciones adicionales cuando se trata de proteger la información. El desarrollo de la seguridad electrónica ha permitido a las organizaciones descubrir una gama más amplia de similitudes entre los ataques que ocurren a través de su entorno de seguridad y el desarrollo de medidas apropiadas para contrarrestarlos. Para

mejorar aún más la seguridad de la información, hay una necesidad de conceptualización de las relaciones entre la seguridad electrónica y los elementos principales que intervienen en la modificación de la infraestructura de una compañía (Smith, 2004). Las organizaciones deben actuar de manera ética, especialmente cuando se trata de las políticas y prácticas de seguridad y de privacidad electrónica.

El presente trabajo de investigación se basa en las siguientes preguntas:

Pregunta 1: ¿Existe alguna forma asequible de identificar las vulnerabilidades y riesgos en los sistemas de información de las organizaciones?

Pregunta 2: ¿Existe alguna forma asequible de prevenir las vulnerabilidades y riesgos en los sistemas de información de las organizaciones?

Pregunta 3: ¿Son los sistemas expertos una solución viable a la supresión de los vulnerabilidades y riesgos en los sistemas de información de las organizaciones, incluyendo las redes y sus estaciones de trabajo?

Limitaciones y Delimitaciones del Estudio

Esta investigación se limitó a la identificación y prevención de vulnerabilidades y riesgos en los sistemas de información de las organizaciones; en especial, de las empresas que forman parte del mundo financiero. Además, de determinar si los sistemas expertos son una solución factible a la eliminación de dichas fallas.

Con el pasar del tiempo, han proliferado las actividades ilegales que ponen en peligro la protección y el buen funcionamiento de los sistemas informáticos. Este hecho, imposibilita generalizar soluciones que puedan resolver los problemas de seguridad informática. Igualmente, el considerar solo a los sistemas expertos pudo no haber sido suficiente para determinar si hay una mayor seguridad con este tipo de programados que con aplicaciones de otro tipo; tales como: los de planificación de recursos empresariales,

sistemas de apoyo de decisiones, y sistemas de información ejecutiva, entre otros. También, se puede dar el caso de que este estudio quede obsoleto en el futuro, tras el avance vertiginoso de la tecnología; donde nuevas tecnologías de informática pueden ser más efectivas y eficaces que las actuales.

Importancia del Estudio

Según estudios antes indicados (Audestad, 2005; Chang y Ho, 2006; Kankanhalli et al., 2003; Knapp et al., 2006; Koskosas y Paul, 2004), la clave para la eficacia de los controles de seguridad informática, requiere la comprensión de los factores tecnológicos, humanos y organizacionales. Dado el caso, es que se decide considerar a los sistemas expertos como una posible solución a la seguridad de las redes de las empresas. De obtener un resultado evidente, se estaría dando un posible impulso al desarrollo de nuevas aplicaciones a éstos programados de alta capacidad de deducción para detectar y prevenir fallas de seguridad. Además, de una debatible reducción de costos de mantenimiento de las redes en las empresas (Firebaugh, 1989).

REVISIÓN DE LITERATURA

Para desarrollar esta investigación, el enfoque se hizo a través de los siguientes temas: las vulnerabilidades y los riesgos en el campo de la informática, y los sistemas expertos como herramienta para erradicar dichas debilidades en los sistemas computadorizados. A continuación, se discute qué son las vulnerabilidades y su impacto en las empresas.

Las Vulnerabilidades

Según Puig (2008), "una vulnerabilidad es la potencialidad o posibilidad de ocurrencia de la realización de una amenaza sobre un activo" (Capítulo 7, p. 1). Para estimar la vulnerabilidad o frecuencia potencial de las amenazas que afectan a cada

activo o grupo de activos, debe participar el responsable y; por tanto, un buen conocedor de cada activo. Que esté suficientemente informado por el especialista para que comprenda o imagine con objetividad la acción potencial de las amenazas. Se suponen tres tipos de vulnerabilidades:

- Vulnerabilidad intrínseca – Si solo depende del activo y de la amenaza.
- Vulnerabilidad efectiva – Es el efecto de la aplicación de las defensas existentes.
- Vulnerabilidad residual – Es la consecuencia de aplicar las defensas complementarias, aconsejadas como resultado del análisis y manejo de riesgos.

Se debe medir la vulnerabilidad, considerando la distancia entre la amenaza potencial y su materialización como agresión real sobre el activo. Siempre que sea posible, se calcula la frecuencia de ocurrencia a partir de hechos objetivos—estadísticas de incidentes o series empíricas. Por ejemplo, una ocurrencia por semana laboral lleva a una frecuencia de 1 en 5 = 0.2; mientras, una ocurrencia por mes laboral da una frecuencia de 1 en 20 = 0.05. El autor señala que se pueden considerar las siguientes frecuencias como correspondencia con las vulnerabilidades. Refiérase a la Tabla 1.

Tabla 1
Relación entre la Frecuencia y la Vulnerabilidad

Rango de Frecuencia	Nivel de Vulnerabilidad
Menor a 1 semana	Muy alto
Menor a 2 meses	Alto
En torno a 1 año	Medio
Menor a 6 años	Bajo
Superior a 6 años	Muy bajo

Determinación de Impacto

El impacto de un activo es la consecuencia sobre éste de la materialización de una amenaza. Es la diferencia en las estimaciones del estado de seguridad del activo obtenidas antes y después de la agresión o materialización de la amenaza sobre éste. Un impacto puede ser cuantitativo (si representa pérdidas económicas) o cualitativo.

El impacto en función de sus consecuencias se puede agrupar en:

- Consecuencias Cualitativas

  Se incluyen conceptos como: inseguridad jurídica, desconfianza, incomodidades, imagen, credibilidad y prestigio, entre otros.

- Consecuencias Cuantitativas

  Se incluyen pérdidas de valor económico, ligadas a activos inmobiliarios. También pérdidas indirectas, valorables económicamente—no registradas. Tales como: gastos de tasación y restauración, reposición de elementos no tangibles del sistema—datos, programas, documentación, procedimientos. Además pérdidas indirectas, valorables económicamente y unidas a disfuncionalidades tangibles. Tales como: perturbación o ruptura de los flujos y ciclos productivos, deterioro de calidad del producto, incapacidad de cumplimentar las obligaciones contractuales. Finalmente, pérdidas económicas relativas a responsabilidad legal—civil, penal o administrativa.

A partir de esta información se procede a valorar el costo económico de un impacto sobre un activo. Puig (2008) señala que se pueden considerar las siguientes escalas para hacer el cálculo cuantitativo de un impacto. Refiérase a la Tabla 2.

Tabla 2
Relación entre el Costo Económico y el Impacto

Rango de Valores (en USD)	Nivel de Impacto
Hasta $1,000	Muy bajo
Entre $1,000 y $10,000	Bajo
Entre $10,000 y $100,000	Medio
Entre $100,000 y $1,000,000	Alto
Superior a $1,000,000	Muy alto

Identificación de las Fuentes de Vulnerabilidad

Las vulnerabilidades de un sistema surgen a partir de errores individuales en un componente, sin embargo nuevas y complejas vulnerabilidades surgen de la interacción entre varios componentes como sistemas de archivos, servidores de procesos, entre otros. Estas vulnerabilidades generan problemas de seguridad para la red y sus estaciones de trabajo (Acosta et al., 2004).

Muchas veces, las personas se han preguntado: ¿cómo puedo defenderme, de algo que no conozco? Para poder uno defenderse, se debe conocer cuáles son las principales vulnerabilidades—o debilidades— en un sistema computadorizado, advirtiendo que es todo dispositivo que integra las comunicaciones, las estaciones de trabajo, las redes, los antivirus, los servidores, los corta fuegos, los programados e individuos, entre otros.

Una vez se conocen cuáles son los componentes de un sistema computadorizado, entonces se puede establecer una serie de recomendaciones para atender los puntos de debilidad que se deben reforzar con: herramientas, mejores prácticas y sobre todo con el conocimiento de que la seguridad solamente puede ser lograda; a través de políticas y

procedimientos, de la tecnología y sobre todo del elemento más importante: el recurso humano, ya que es la principal vulnerabilidad en cualquier sistema.

Los sistemas de información computarizados son vulnerables a una diversidad de amenazas y atentados por parte de: personas tanto internas como externas de la organización; desastres naturales; servicios, suministros y trabajos no confiables e imperfectos; la incompetencia y las deficiencias cotidianas; el abuso en el manejo de los sistemas informáticos; por el desastre a causa de intromisión, robo, fraude, sabotaje o interrupción de las actividades de automatizaciones.

A continuación, se discute qué son los riesgos y cuáles son las amenazas qué pueden afectar el desempeño de las organizaciones.

LOS RIESGOS

Los riesgos son amenazas que atentan contra la vulnerabilidad en seguridad de la organización o sus recursos (Cintrón, 2006). Los estudios y estadísticas sobre seguridad en el manejo de sistemas de información confirman que la mayoría de sus malos usos provienen de la propia organización, aunque también están sometidos a amenazas externas (Websense Inc., 2007). Las amenazas principales son:

- Amenazas Internas

  Éstas incluyen la divulgación de información confidencial por los trabajadores de la empresa; el envío de mensajes difamatorios bajo direcciones de correos electrónicos corporativas; y el uso de los sistemas corporativos para la descarga ilegal de obras o almacenamiento de contenidos ilícitos.

- Amenazas externas

Éstas incluyen los accesos no autorizados a los sistemas de información corporativos; el acceso no autorizado a secretos industriales e información confidencial—intrusión, antiespías, entre otros, la inutilización de los sistemas de información por ataques externos—virus, denegaciones de servicio, entre otros; los fraudes—"phishing", divulgación de claves de acceso, entre otros; y el uso de los sistemas corporativos por elementos externos para ataques a sistemas informáticos de terceros.

Prevención

La seguridad informática es una disciplina que se relaciona a diversas técnicas, aplicaciones y dispositivos encargados de asegurar la integridad y privacidad de la información de un sistema computadorizado y sus usuarios. Entonces, ¿cómo podemos prevenir los riesgos en el diseño de la tecnología, si es posible que nunca se hayan visto riesgos similares antes? ¿Qué tan probable son los eventos futuros asociados? ¿Puede un riesgo ser expresado objetivamente? Tales cuestionamientos filosóficos sobre el riesgo han estado planteándose por un tiempo (Cross, 1992; Jasanoff, 1998; Shrader Frechette, 1990). Estas preguntas también se han discutido en el contexto de la crítica a las teorías clásicas de evaluación de la tecnología, donde se señala que el futuro tiene demasiadas variables para permitir obtener una confiabilidad o, incluso una aproximación de las predicciones en el futuro. También, se ha mencionado que los modelos que no tienen en cuenta las complejidad de la incorporación social (Adams, 1995; Bradbury, 1989; Pursell, 1979).

Con la aparición del nuevo campo de la seguridad informática, la objetividad de riesgo y la seguridad a menudo se asume implícitamente (Evans y Paul, 2004; Nikander y Karvonen, 2001; Pieters, 2006; Riedl, 2004; Xenakis y Macintosh, 2005), pero preguntas similares pueden plantearse sobre la incertidumbre en la evaluación de estas variables.

La posibilidad de comportamiento intencional por un atacante para hacer que el sistema falle, aumenta la incertidumbre en el caso de la seguridad; ya que la predicción de lo que los seres humanos pueden hacer se piensa que es diferente de la predicción de lo que la naturaleza puede hacer. No es una doble contingencia, y el juego de las vulnerabilidades es un acto de comunicación entre los atacantes y defensores (Luhmann, 1995).

Factores de Riesgos

Los factores de riesgos pueden clasificarse en: factores humanos, factores organizacionales y factores tecnológicos. A continuación, una descripción de cada uno de ellos.

Factores humanos

Desde el punto de vista humano, la adopción de prácticas de seguridad plantea varios desafíos para los profesionales de la seguridad. Por ejemplo, las interacciones efectivas y las comunicaciones son necesarias para alcanzar un entendimiento mutuo sobre los riesgos de seguridad entre las diferentes partes interesadas. Koskosas y Pablo (2004) estudiaron cómo se comunican los riesgos de seguridad en las organizaciones financieras. Ellos concluyen que la comunicación de riesgos tiene un rol importante a nivel macro de la gerencia de seguridad y que afecta a la configuración de los objetivos de seguridad de la banca.

Por su parte, Tsohou et al. (2006) reconocen que el manejo del riesgo es básicamente una actividad humana y proponen el uso de la teoría cultural para clasificar las diferentes percepciones de los riesgos de seguridad que los interesados puedan tener. Dependiendo de la clasificación, profesionales de la seguridad deben adoptar estrategias diferentes para comunicarse y llegar a las percepciones de riesgos comunes con otras partes interesadas.

Mientras, Garigue y Stefaniu (2003) elaboraron sobre la importancia de la presentación de informes con el fin de comunicar sus preocupaciones de seguridad en las organizaciones. Llegan a la conclusión de que la presentación de informes sobre cuestiones de seguridad es una ciencia y un arte, con mucho juicio humano necesario para interpretar los informes de las herramientas de seguridad.

Los errores humanos representan otra amenaza para las mejores prácticas de seguridad. Kraemer y Carayon (2007) definen error humano como causa accidental de humanos, pero no intencional de equipos pobres y seguridad de la información (por ejemplo, un error de programación accidental que causa una computadora se cuelgue en determinadas circunstancias). Los autores identifican y caracterizan los elementos relacionados con errores humanos en el ámbito de la seguridad de la información. Se completa un marco conceptual con los datos cualitativos a partir de 16 entrevistas con los administradores de red y especialistas en seguridad. Su análisis muestra que los factores de organización como la comunicación, la cultura de seguridad, y la política son causa frecuente de errores en el contexto de seguridad de la información y que interrupciones en la comunicación causan vulnerabilidades de seguridad.

Factores organizacionales

Kankanhalli et al. (2003) proponen un modelo que relaciona los factores organizacionales; tales como tamaño de la organización, el apoyo a la alta gerencia, y el tipo de industria con la eficacia de los controles de seguridad de la información en las organizaciones. De 63 encuestados, ellos concluyeron que el apoyo de la gerencia se relaciona positivamente con la aplicación de medidas de seguridad preventiva. También, encontraron que las entidades financieras invierten más recursos en los controles para impedir las malas prácticas de seguridad que otras organizaciones y que las

organizaciones más grandes invierten más dinero en medidas de disuasión que las más pequeñas.

Del mismo modo, Chang y Ho (2006) estudiaron los factores que influyeron en la adopción de las normas de seguridad "TI BS7799" en diversas organizaciones en Taiwán. De 59 encuestados, también se desprende que los factores como el apoyo de la alta gerencia, el tamaño y tipo de organización están relacionados con la aplicación de controles de seguridad. Además, sus hallazgos sugieren que la incertidumbre de los elementos del medio ambiente; tales como el cambio rápido de la tecnología, el comportamiento de los competidores, los requisitos de seguridad de los clientes y los cambios en la legislación afectan la administración de la seguridad.

Knapp et al. (2006) encuestaron a 936 profesionales de la seguridad acerca de la importancia del apoyo de la alta gerencia en la predicción del manejo de políticas y la cultura de seguridad dentro de las organizaciones. Los autores llegaron a la conclusión de que este factor es fundamental para la aplicación de controles de seguridad dentro de las organizaciones. Del mismo modo, Straub y Welke (1998) estudiaron el impacto del adiestramiento de la gerencia sobre la implantación de los planes de seguridad en dos organizaciones de servicios técnicos. Éstos llegaron a la conclusión de que los administradores no están conscientes de todo el espectro de acciones que se pueden tomar para reducir los riesgos, pero que emplearían técnicas de planificación para la seguridad si son adiestrados en los mismos

Factores tecnológicos

La complejidad tecnológica es otro desafío para los profesionales de la seguridad. Según Audestad (2005), una de las razones para no alcanzar el 100 por ciento de seguridad se debe a la complejidad de la tecnología. Esta complejidad hace que sea muy

difícil tomar decisiones para manejar todo el escenario y, a la vez, diseñar las políticas de seguridad que cubran todas las posibles configuraciones de los sistemas.

Por otro lado, Jiwnani y Zelkowitz (2002) describen las pruebas de seguridad de los sistemas como un proceso largo, complejo y costoso. Proponen una disposición para clasificar las vulnerabilidades y los riesgos; y así, ayudar a los profesionales de la seguridad en establecer un orden para asegurar los recursos informáticos.

A continuación, se discute qué son los sistemas expertos y cómo pueden contribuir para mejorar la seguridad en los sistemas de información de las empresas.

LOS SISTEMAS EXPERTOS

El concepto del sistema experto se basa en el supuesto de que el conocimiento de un experto se puede almacenar en una computadora y, luego se aplica por otros usuarios cuando sea necesario. Un sistema experto ofrece capacidades únicas, al igual que un sistema de apoyo de decisiones. En primer lugar, un sistema experto ofrece la oportunidad de tomar decisiones que exceden las capacidades del gerente. Por ejemplo, un oficial nuevo de inversiones de un banco puede utilizar un sistema experto diseñado por un gran conocedor financiero e incorporar los conocimientos del experto en sus decisiones de inversión. En segundo lugar, el sistema experto puede explicar su razonamiento para llegar a una solución particular. Por lo general, la explicación de cómo se llegó a una solución es más valioso que la propia solución.

Davis (1984) indica las características de los sistemas basados en el conocimiento para establecer un conjunto de principios arquitectónicos: el conocimiento es la clave para el poder de los sistemas expertos, el conocimiento es a menudo inexacto e incompleto, el conocimiento es a menudo mal especificado, los novatos se convierten en expertos de forma incremental, el sistema experto debe ser flexible y, el sistema experto

debe ser transparente. Mientras, Firebaugh (1989) menciona que algunos de los principios generalmente aceptados para la construcción de los sistemas expertos son: en primer lugar, separar el motor de inferencia y el banco de conocimientos. Él indica, "una clara separación del motor de inferencia y del banco de conocimientos ayuda a evitar la duplicación y la reducción de la eficiencia del programa." En segundo lugar, utilizar una representación lo más uniforme posible. El autor concluye que a mayor cantidad de representaciones de conocimiento o excepciones a las reglas de inferencia se añaden, menor será el funcionamiento real del sistema, por lo que lo haría inmanejable. En tercer lugar, se debe mantener el motor de inferencia simple. Él afirma, que con un motor de inferencia simple es más fácil saber qué conocimiento se va a utilizar para mejorar el rendimiento del sistema. Por último, explotar la redundancia. Se debe recopilar la mayor cantidad posible de información de un problema particular para garantizar una solución lo más precisa posible.

Comparación con otras Tecnologías de Información

Como ocurre con muchas otras tecnologías, hay un lapso de tiempo considerable entre la adopción de la tecnología de sistemas expertos y en los beneficios derivados de la utilización para las organizaciones (Lu y Guimaraes, 1988). La literatura tiene una abundancia de estudios de evaluación de la implantación de sistemas para computadoras. Lamentablemente, la gran mayoría de los estudios están relacionados con los sistemas de procesamiento de transacciones, sistemas de apoyo de decisiones, sistemas de información ejecutiva, y otros sistemas de información a parte de los sistemas expertos. El término sistema experto se refiere a los sistemas que comprenden; al menos, un banco de conocimientos, un motor de inferencia, un módulo de explicación, y una interfaz de usuario con el fin de imitar a expertos en la toma de decisiones (Jih, 1990). Aunque

obviamente hay muchas similitudes, los sistemas expertos son muy diferentes de otros sistemas en muchas maneras. Por ejemplo, la base de un sistema experto es la captura y uso del conocimiento de expertos de alto nivel para ayudar a los usuarios menos competentes. El acuerdo de otros sistemas con el flujo de datos e información a través de la unidad de organización, y su desarrollo requiere una considerable aportación de los usuarios para definir la naturaleza, funciones y características del sistema. Por tanto, para los sistemas de procesamiento de transacciones, sistemas de apoyo de decisiones y sistemas de información ejecutiva, los usuarios son los "expertos del dominio".

Los sistemas expertos también son dramáticamente diferentes de otros tipos de programados. Por ejemplo, los sistemas de procesamiento de transacciones se centran en el procesamiento de datos de rutina y en los procesos de negocio. Mientras, los sistemas de apoyo de decisiones se centran en los modelos de cálculo y estadística. Por otra parte, mientras que los sistemas expertos también pueden realizar o apoyar las decisiones, se centran en el conocimiento y experiencia, y no en el procesamiento de transacciones o de técnicas de cálculos (Duda y Shortliffe, 1983). Los sistemas expertos son particularmente viables para los problemas que no pueden ser resueltos mediante algoritmos (Writzel y Kerschberg, 1989).

Según Jih (1990), se ha encontrado diferencias entre los sistemas expertos y los sistemas de procesamiento de transacciones a lo largo de las siguientes áreas: misión primordial, definición de la estructura del conocimiento, requisitos de seguridad e integridad de los datos entrados, capacidad del sistema para compartir, interfaz para los usuarios con los sistemas, extracción de datos y validación. Mientras, Turban y Watkins (1986) examinaron las diferencias entre los sistemas de apoyo de decisiones y los sistemas expertos, a lo largo de los siguientes atributos: objetivos, quién toma las

decisiones, orientaciones principales, dirección de consulta más importantes, naturaleza del apoyo, método de manipulación de datos, características de las zonas problema, repetición de los problemas tratados, contenido de los bancos de datos, capacidad de razonamiento, y capacidad de explicación. Posteriormente, Turban (1990) analizó las diferencias entre los sistemas de procesamiento de transacciones, los sistemas de información gerencial, los sistemas de apoyo de decisiones, los sistemas de información ejecutivos y los sistemas expertos; en términos de tipos de aplicaciones, enfoque de apoyo, naturaleza de los bancos de datos, capacidades de apoyo a la toma de decisiones, manipulación numérica frente a la simbólica, tipos de información producida , nivel más alto de la organización apoyada e impulso primario para el sistema.

Herramienta de Prevención

Los sistemas expertos pueden obtener y desarrollar suficiente conocimiento mediante las inferencias que hacen, como para identificar y prevenir las vulnerabilidades y riesgos a los sistemas de información. Según Cintrón (s.f.), se debe establecer una verificación de la seguridad de los activos informáticos de la organización. Para ello, es recomendable hacer una hoja de cotejo. Refiérase a la Tabla 3.

La Tabla 3, puede ayudar a desarrollar un sistema experto que incluya cada uno de los ítems y sus sub-ítems con sus respectivas características, asociarlos con sus respectivas áreas y determinar si están disponibles o no. Si están disponibles, entonces verificar si están actualizados o si se necesita establecer nuevos conceptos, procedimientos, reglas de inferencia, métodos de razonamiento y restricciones. Finalmente, indicar la fecha de la más reciente revisión. Este proceso permite expandir el conocimiento, previamente adquirido y lo entrelaza para crear nuevas deducciones que buscan solucionar el problema identificado.

Tabla 3
Hoja de Cotejo para Verificar la Seguridad de los Activos Informáticos

Área	Ítem	¿Está disponible y actualizado?	Fecha última revisión
Organización	Organigrama		
	Descripción de plazas		
	Objetivos y servicios		
	Plano físico del área		
Planificación	Plan estratégico		
	Plan de sustitución tecnológica		
	Plan de trabajo		
	Presupuesto		
	Informes de progreso		
Inventario	Equipo – "hardware"		
	Equipo – red		
	Programación y licencias		
	Otros componentes físicos		
Operaciones	Lista de aplicaciones		
	Descripción de cada aplicación y documentación		
Desarrollo y Mantenimiento	Solicitud de servicios		
	Trámite solicitud		
	Forma de modificación de programas o sistemas		
	Forma de aprobación e instalación		
Bitácoras	Trabajos/Procesos		
	Acceso físico		
	Acceso a la red		
	Acceso a aplicaciones (usuarios)		
	Control		
	Itinerario de operaciones		
	Itinerario de tareas		
	Resguardos		
Planificación de Contingencias	Comité de respuesta a emergencias		
	Plan de recuperación de desastres		
	Acuerdos de operación alterna		
	Adiestramientos y simulacros		
Seguridad	Plan de seguridad		
	Arquitectura de seguridad		
	Políticas y procedimientos		
	Fundamentos		
	Bitácoras		
	Medidas de control de seguridad		

METODOLOGÍA

Construcción del Sistema Experto propuesto

Si se utiliza como base la Tabla 3 - Hoja de Cotejo para Verificar la Seguridad de los Activos Informáticos para desarrollar el sistema experto para prevenir las vulnerabilidades y riesgos en los sistemas informáticos, entonces se tiene que construir el conocimiento de los siguientes elementos. Refiérase a la Figura 1.

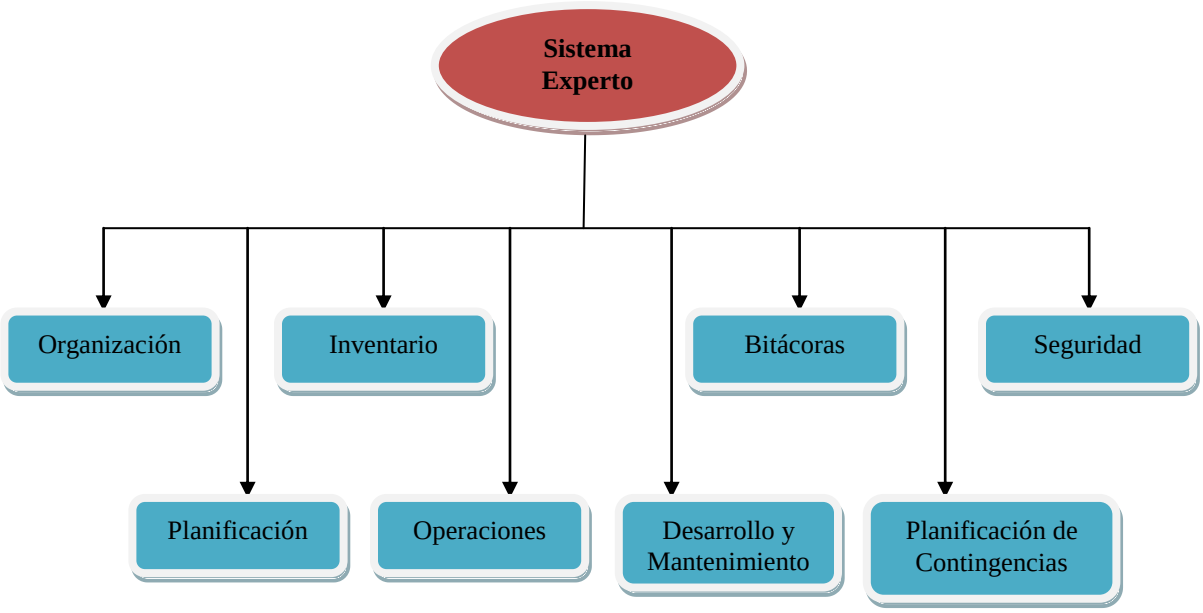

Figura 1. **Diagrama de los Elementos Claves para desarrollar el Sistema Experto propuesto**

Comenzamos por identificar y codificar cada ítem asociado con la Organización y, sus respectivos procedimientos, reglas de inferencia, casos especiales, métodos de razonamiento, y restricciones, entre otros para expandir y actualizar el conocimiento. Refiérase a la Figura 2.

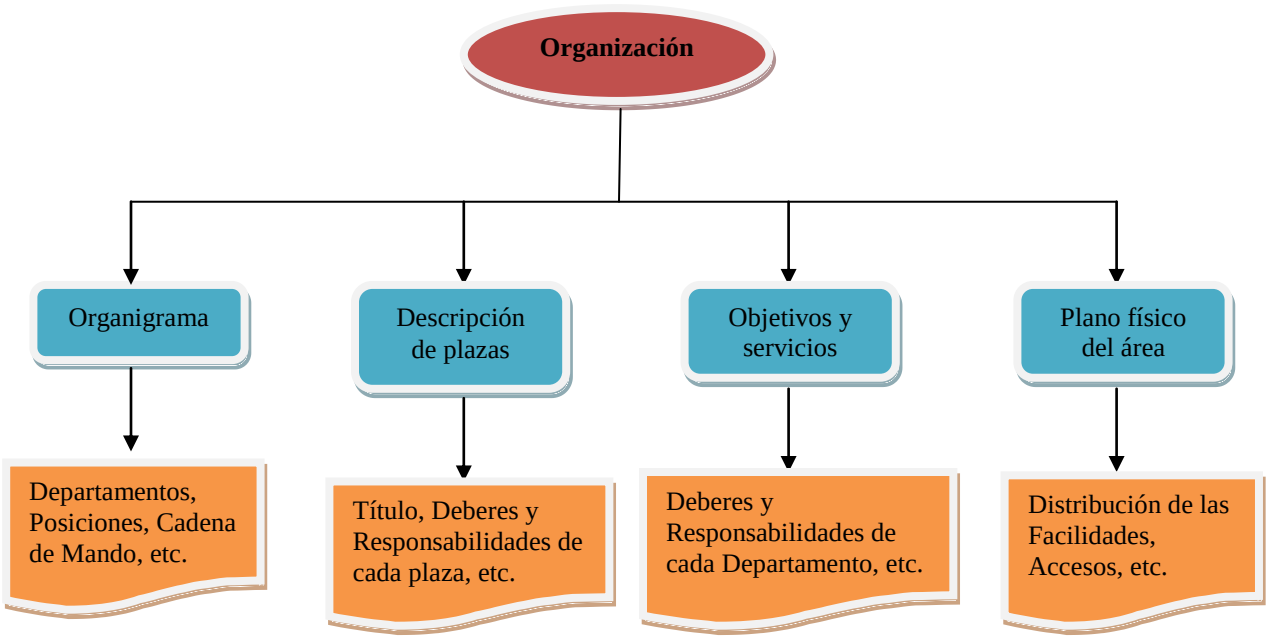

Figura 2. **Diagrama de los Ítems asociados a la Organización**

Luego, se procede a identificar y codificar cada ítem asociado con la Planificación y, sus respectivos procedimientos, reglas de inferencia, casos especiales, métodos de razonamiento, y restricciones, entre otros para expandir y actualizar el conocimiento. Refiérase a la Figura 3.

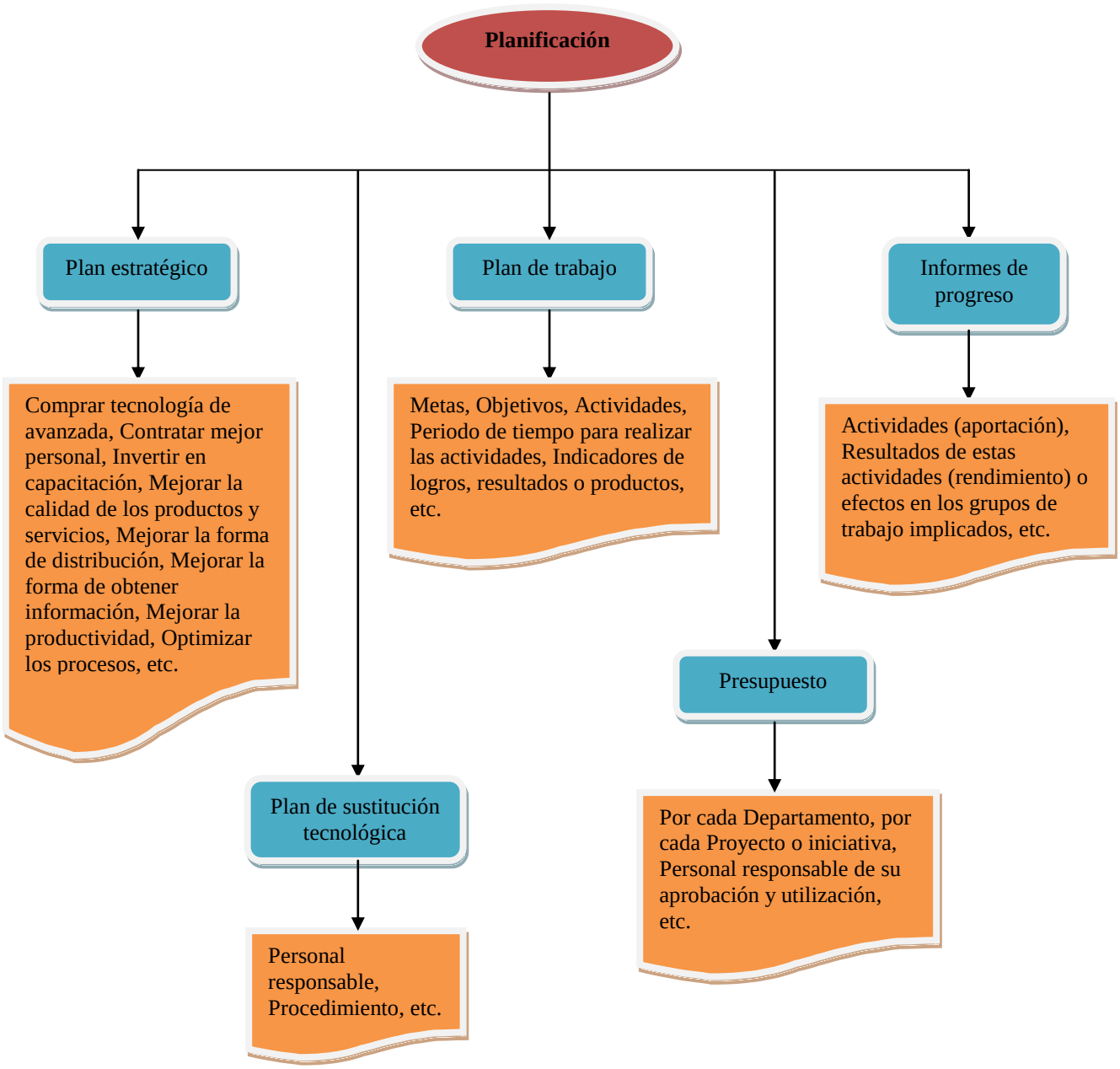

Figura 3. **Diagrama de los Ítems asociados a la Planificación**

Continuando, se procede a identificar y codificar cada ítem asociado con el Inventario y, sus respectivos procedimientos, reglas de inferencia, casos especiales, métodos de razonamiento, y restricciones, entre otros para expandir y actualizar el conocimiento. Refiérase a la Figura 4.

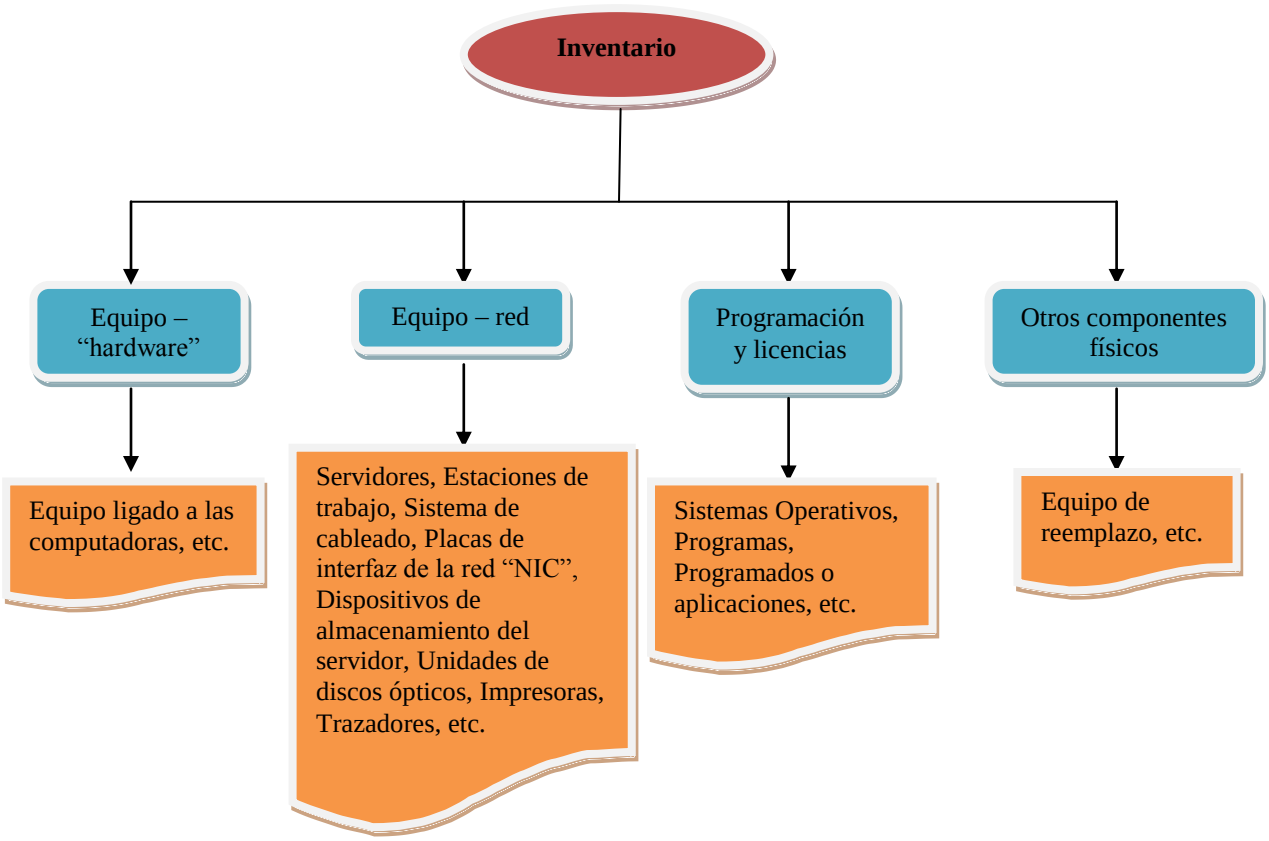

Figura 4. **Diagrama de los Ítems asociados al Inventario**

Repitiendo, se procede a identificar y codificar cada ítem asociado con las Operaciones y, sus respectivos procedimientos, reglas de inferencia, casos especiales, métodos de razonamiento, y restricciones, entre otros para expandir y actualizar el conocimiento. Refiérase a la Figura 5.

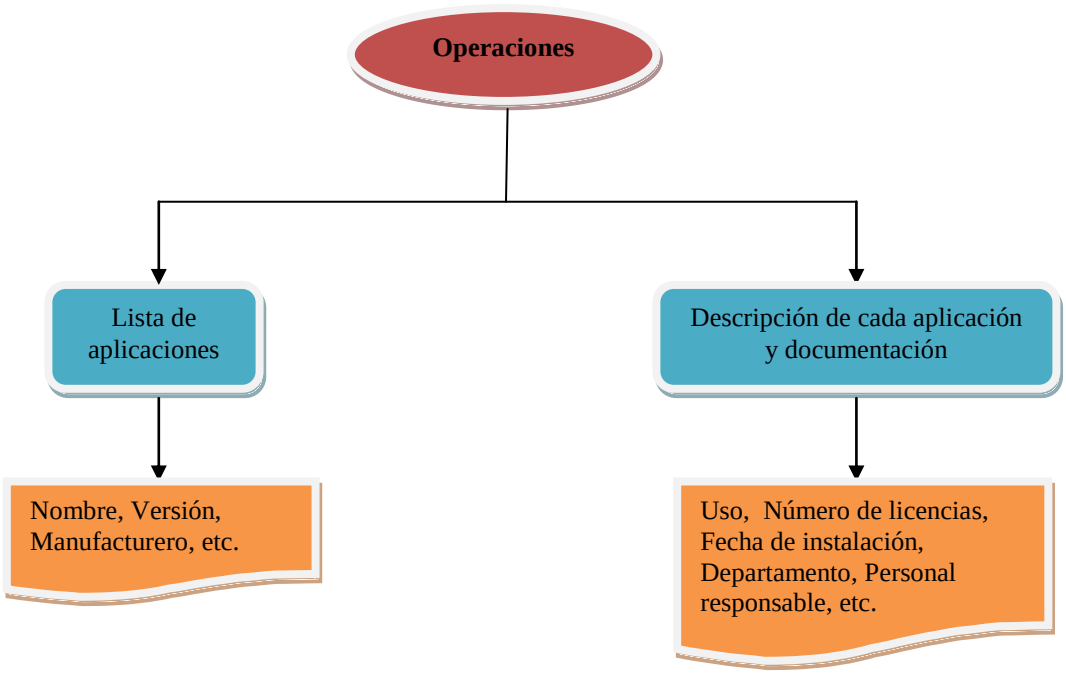

Figura 5. **Diagrama de los Ítems asociados a las Operaciones**

Prosiguiendo, se identifica y codifica cada ítem asociado con el Desarrollo y Mantenimiento y, sus respectivos procedimientos, reglas de inferencia, casos especiales, métodos de razonamiento, y restricciones, entre otros para expandir y actualizar el conocimiento. Refiérase a la Figura 6.

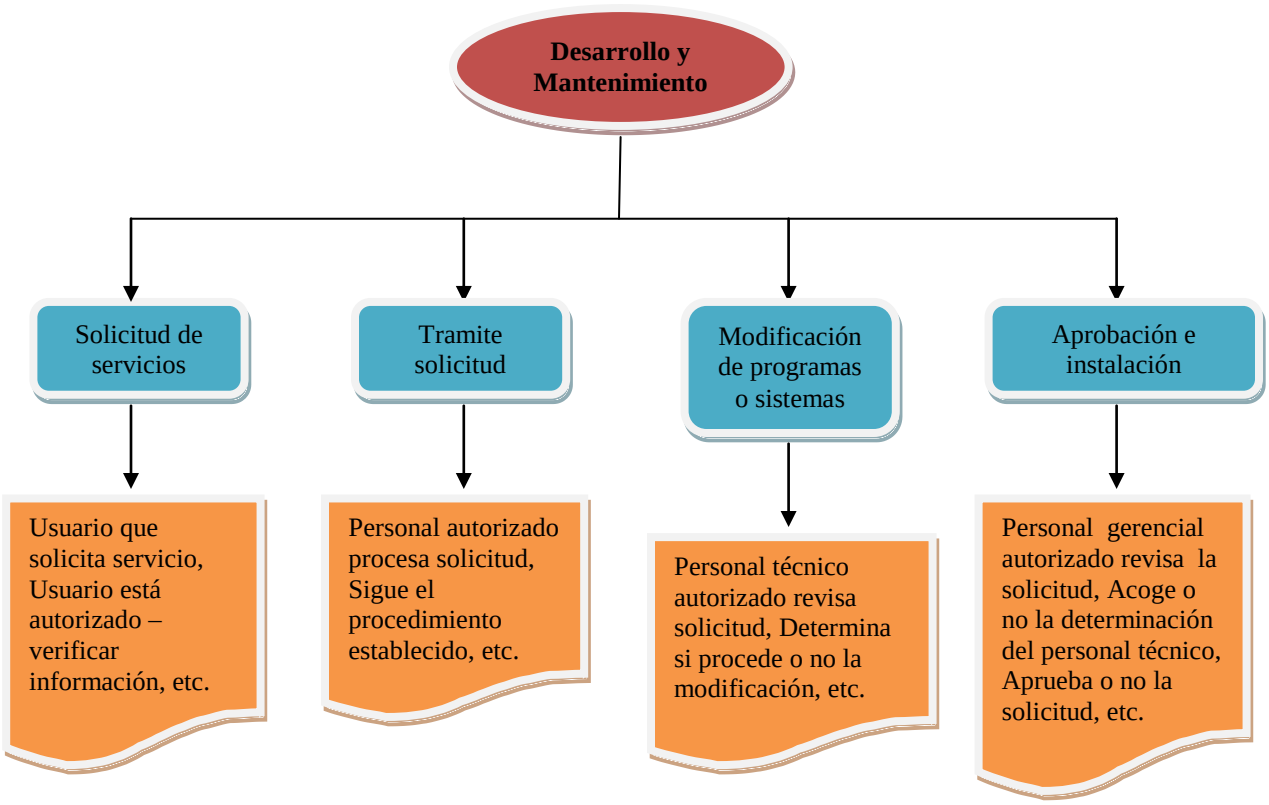

Figura 6. **Diagrama de los Ítems asociados al Desarrollo y Mantenimiento**

Adelantando, se identifica y codifica cada ítem asociado con las Bitácoras y, sus respectivos procedimientos, reglas de inferencia, casos especiales, métodos de razonamiento, y restricciones, entre otros para expandir y actualizar el conocimiento. Refiérase a la Figura 7.

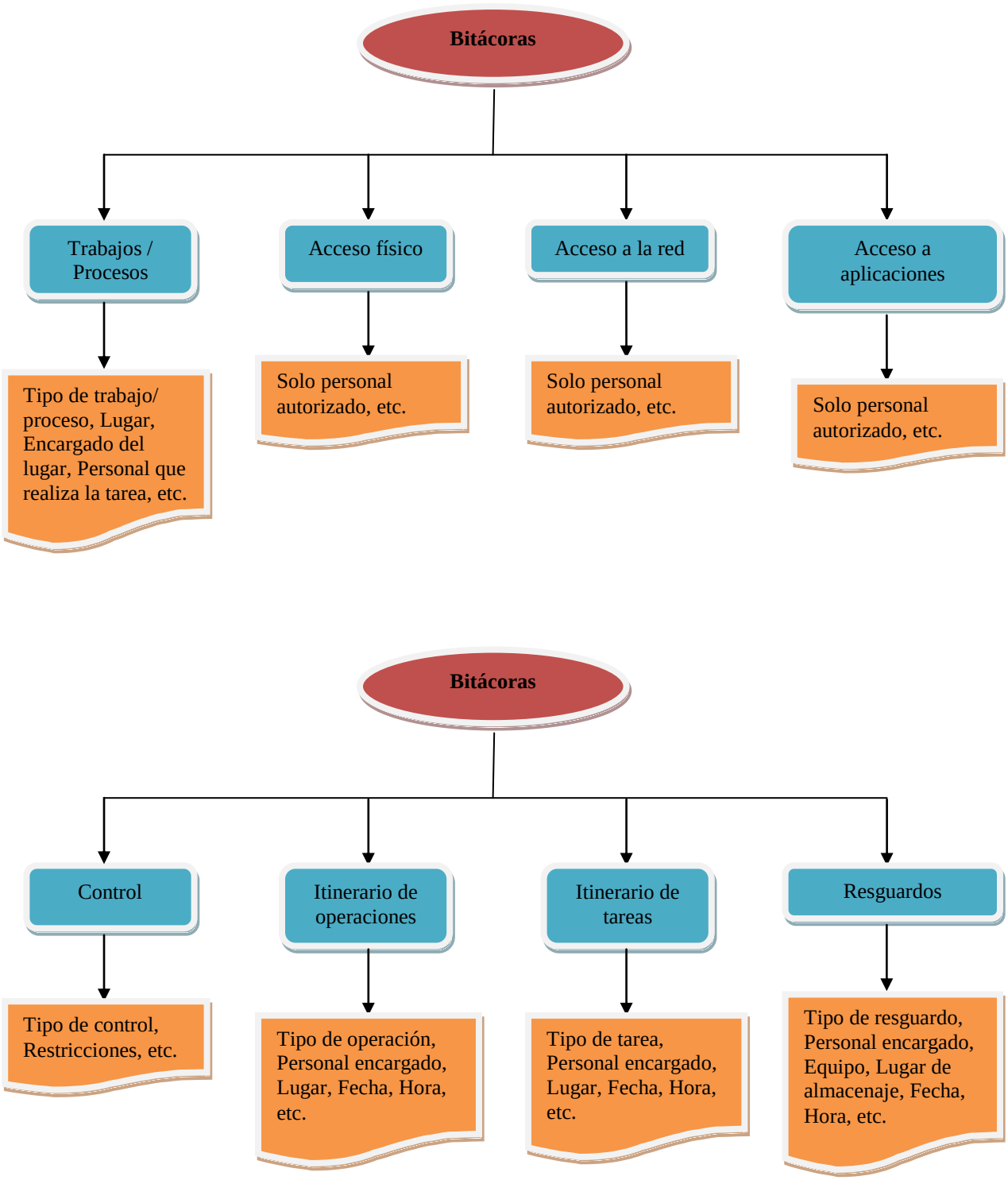

Figura 7. **Diagrama de los Ítems asociados a las Bitácoras**

Luego, se procede a identificar y codificar cada ítem asociado con la Planificación de Contingencias y, sus respectivos procedimientos, reglas de inferencia, casos especiales, métodos de razonamiento, y restricciones, entre otros para expandir y actualizar el conocimiento. Refiérase a la Figura 8.

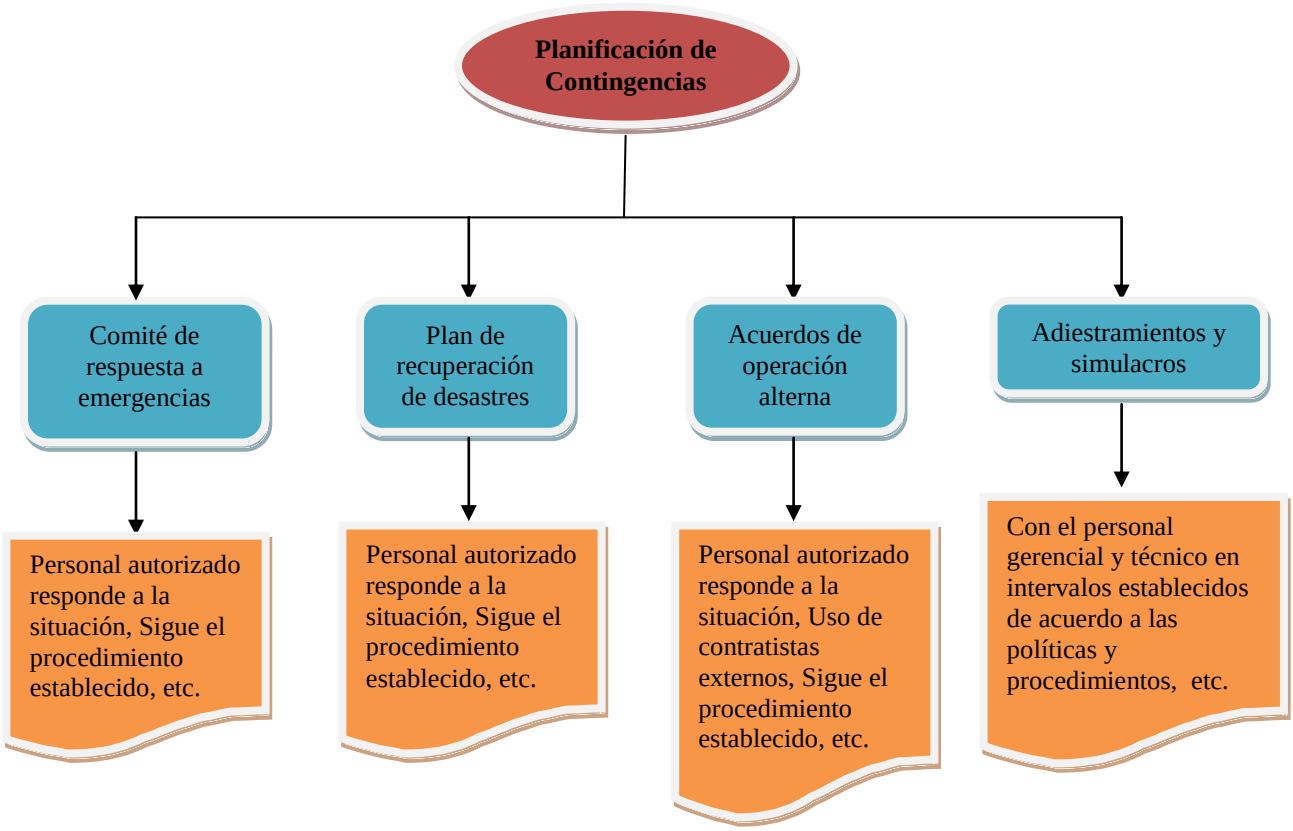

Figura 8. **Diagrama de los Ítems asociados a la Planificación de Contingencias**

Finalmente, se procede a identificar y codificar cada ítem asociado con la Seguridad y, sus respectivos procedimientos, reglas de inferencia, casos especiales, métodos de razonamiento, y restricciones, entre otros para expandir y actualizar el conocimiento. Refiérase a la Figura 9.

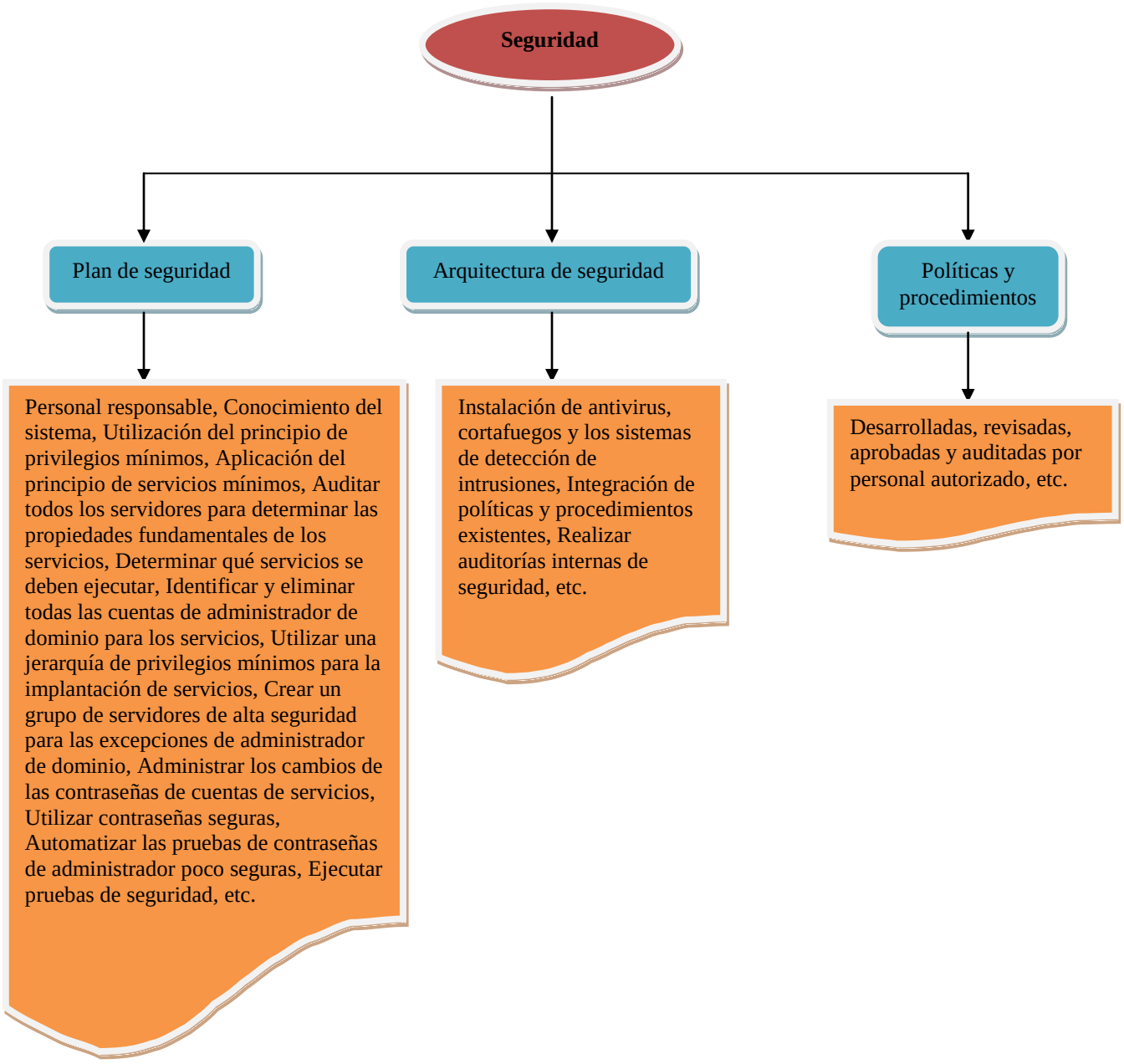

Figura 9(a). **Diagrama de los Ítems asociados a la Seguridad**

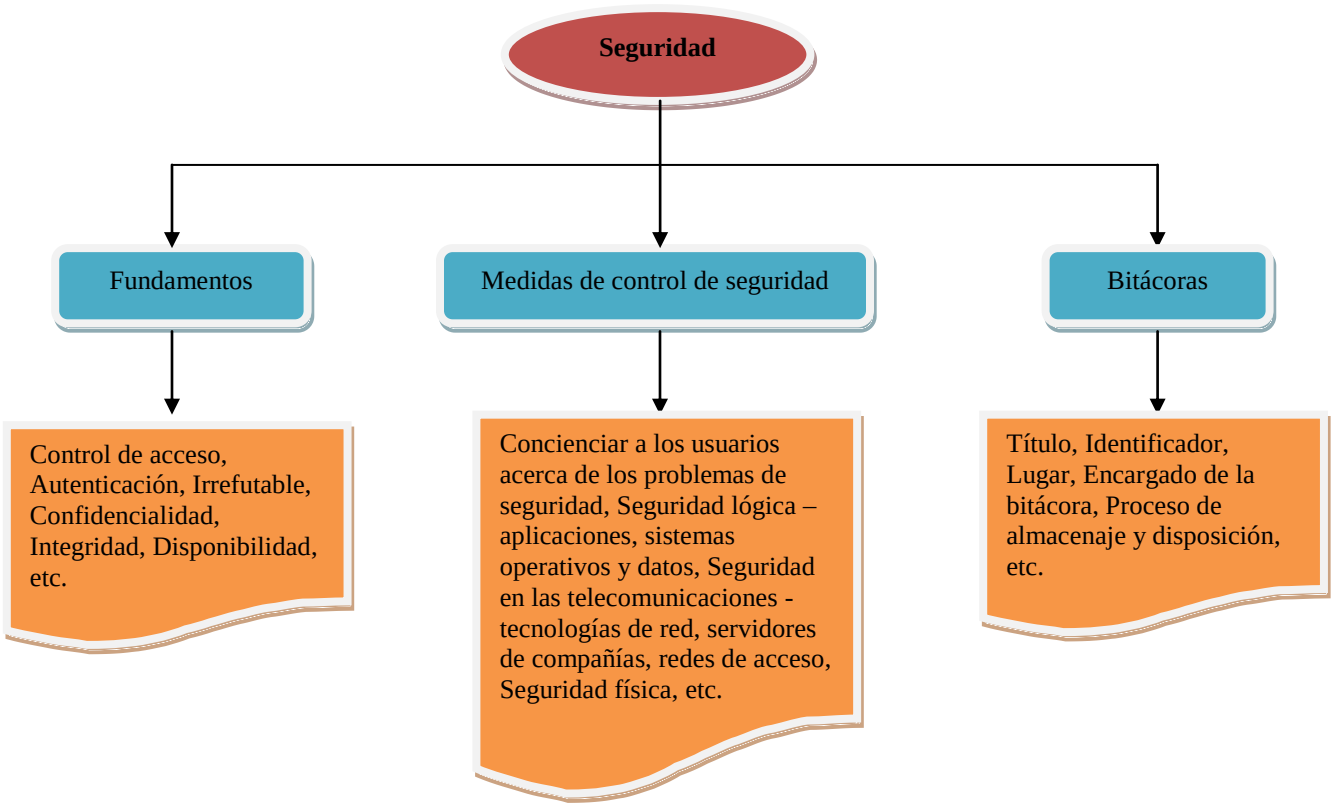

Figura 9(b). **Diagrama de los Ítems asociados a la Seguridad (continuación)**

Con el conocimiento dado a cada uno de los ítems de cada elemento asociado a la seguridad informática, se pretende dar los pasos para desarrollar un sistema experto lo suficientemente robusto como para lograr las metas y objetivos establecidos— identificación y prevención de vulnerabilidades y riesgos en los sistemas de información.

HALLAZGOS

Los hallazgos de esta investigación se apoyaron en el análisis de varios estudios empíricos reconocidos en la literatura. Dada la naturaleza diferente de los sistemas expertos, los resultados obtenidos de estudios anteriores pueden proporcionar una mejor visión de las principales interrogantes que rodean el desarrollo de estos sistemas y su aplicación en la práctica.

Hay varias razones de por qué los estudios que tratan específicamente de los sistemas expertos son importantes:

- A pesar del uso generalizado y de la importancia de la tecnología de los sistemas expertos, poco esfuerzo se ha hecho para probar empíricamente la contribución a sus organizaciones.
- Los administradores responsables del desarrollo y aplicación de los sistemas expertos no pueden asumir que el conjunto de factores determinantes para el éxito de otros tipos de sistemas son igualmente importantes para los sistemas expertos.
- Muchos factores importantes son exclusivos de los sistemas expertos. Es decir, están orientados a los problemas de dominio de la gerencia; las características de los sistemas expertos; las características de los expertos del dominio y de los ingenieros de conocimiento y su relación única con los usuarios.
- Los informes sobre el desempeño de los sistemas expertos (Barsanti, 1990; Ignizio, 1991; Keyes, 1989; O'Neal, 1990; Prerau, 1990; Smith, 1988) se basan principalmente en la opinión y la experiencia personal de un individuo y no han sido empíricamente probado. Los estudios

empíricos realizados por Byrd (1992); y Tyran y George (1993) informan sobre preguntas generales y los factores que rodean las aplicaciones de los sistemas expertos. Pero en las investigaciones se necesita mucho más para formular y someter a prueba hipótesis sobre la percepción que tienen los administradores y usuarios sobre el rol y contribución de los sistemas expertos en la identificación y prevención de las vulnerabilidades y riesgos a que están expuestos los sistemas informáticos de las organizaciones.

Respuestas a las Preguntas del Estudio

Este trabajo de investigación exploratorio basó su análisis en las siguientes preguntas:

Pregunta 1: ¿Existe alguna forma asequible de identificar las vulnerabilidades y riesgos en los sistemas de información de las organizaciones?

Según lo examinado, se puede responder en la afirmativa. Pero, mediante una evaluación exhaustiva previa a la implantación de un sistema. Esta evaluación, conocida como evaluación de riesgos, es un proceso vital en cualquier desarrollo eficaz de un sistema de información. De hecho, los riesgos son inherentes a cualquier iniciativa y son un componente necesario en la toma de decisiones. Según Nunes y Annansingh (2002), un mal manejo de los riesgos en un proyecto a menudo conduce al fracaso y, esto no es una situación poco común en los sectores público y empresarial. Entre otras causas, las fallas se han relacionado con las estrategias de negocios y riesgos inadecuadas, basadas en información incompleta y sin la debida autorización de la alta gerencia de la organización. Además, la situación se ve aumentado por la ausencia de definir claramente los límites de riesgos que está dispuesta a asumir; informes deliberadamente malinterpretados; comunicación inadecuada sobre las vulnerabilidades y riesgos dentro

de la organización; control de riesgos superficiales o poco realistas; escaso conocimiento del entorno de la empresa; y la falta de toma de decisiones oportuna.

Pregunta 2: ¿Existe alguna forma asequible de prevenir las vulnerabilidades y riesgos en los sistemas de información de las organizaciones?

Basado en lo hallado en la literatura, se pueden prevenir. Como, por ejemplo, mediante pruebas de penetración (Hauttech Group Ltda., 2010). En los complejos ambientes de redes actuales, las posibilidades de ataques a los sistemas informáticos son cada vez mayores y para mitigar el peligro al que está expuesta la información, es necesario conocer todas las debilidades de las estructuras que las defienden. Para esto se utilizan las pruebas de penetración, que permiten a las organizaciones evaluar proactivamente las vulnerabilidades, usando metodologías y técnicas del mundo real; simulando una intervención en los sistemas de la misma forma en que un atacante lo haría, tanto dentro como fuera de la institución. Además, permite ahorrar tiempo al descartar falsos positivos que no representan debilidades explotables ni riesgos auténticos para la información. Las pruebas de penetración pueden ser consideradas como una buena herramienta para determinar la eficacia de las soluciones de seguridad y los sistemas de defensa, porque analizan activamente si es que tales protecciones pueden ser eludidas por los atacantes.

El aspecto más relevante es que los resultados de las pruebas de penetración permiten al personal de informática identificar las áreas críticas de seguridad que requieren atención inmediata, entre ellas, las vulnerabilidades que pueden ser vistas y explotadas por individuos no autorizados, “crackers”, agentes de información, ladrones, antiguos empleados, competidores, entre otros. Conocer las debilidades de los sistemas

de seguridad posibilita delinear un orden de prioridad frente a aquellos temas que significan riesgos menores.

Pregunta 3: ¿Son los sistemas expertos una solución viable a la supresión de los vulnerabilidades y riesgos en los sistemas de información de las organizaciones, incluyendo las redes y sus estaciones de trabajo?

Se puede aseverar que sí, de vencerse las críticas a los sistemas expertos; tales como sus costos de implantación y la falta de comprensión por parte de sus administradores y usuarios (Gill, 1995). Siguiendo la metodología descrita en el capítulo anterior, se puede desarrollar un sistema de información que identifique y prevenga; por sí solo, las vulnerabilidades y riesgos.

Por ejemplo, al utilizar de base la Tabla 3 se comienza a obtener el conocimiento de un experto en el área de seguridad de los sistemas tecnológicos. Comenzando con la organización: se debe identificar las características del organigrama; de descripción de los puestos; de objetivos y servicios de la empresa; y del plano físico del área. Así, se va adquiriendo nuevo conocimiento de cada elemento (ítem) para hacer una representación e implantación de éstos, mediante reglas; y finalmente, hacer la validación, mediante pruebas para actualizar las características de cada elemento identificado para la organización.

De igual forma, se debe seguir estos pasos para la planificación. Se debe identificar las características del plan estratégico; del plan de sustitución tecnológica; del plan de trabajo; del presupuesto; y de los informes de progreso. Así, se va adquiriendo nuevo conocimiento de cada elemento para hacer una representación e implantación de éstos, mediante reglas; y finalmente, hacer la validación, mediante pruebas para actualizar las características de cada elemento identificado para la planificación.

Luego, se siguen los mismos pasos para el inventario. Se identifican las características del equipo – "hardware"; del equipo de la red; de la programación y sus licencias; y de otros componentes físicos. Así, se va adquiriendo nuevo conocimiento de cada elemento para hacer una representación e implantación de éstos, mediante reglas; y finalmente, hacer la validación, mediante pruebas para actualizar las características de cada elemento identificado para el inventario.

Al continuar con el desarrollo del sistema experto, se sigue la misma metodología para las operaciones. Se identifican las características de la lista de aplicaciones; y la descripción de cada aplicación y documentación. Así, se va adquiriendo nuevo conocimiento de cada elemento para hacer una representación e implantación de éstos, mediante reglas; y finalmente, hacer la validación, mediante pruebas para actualizar las características de cada elemento identificado para las operaciones.

Se prosigue con el método establecido para el desarrollo y mantenimiento. Se identifican las características de la solicitud de servicios; del trámite de la solicitud; de la forma de modificación de programas o sistemas; y de la forma de aprobación e inspección. Así, se va adquiriendo nuevo conocimiento de cada elemento para hacer una representación e implantación de éstos, mediante reglas; y finalmente, hacer la validación, mediante pruebas para actualizar las características de cada elemento identificado para el desarrollo y mantenimiento.

Luego, se continúa con las bitácoras. Se identifican las características de los trabajos o procesos; del acceso físico; del acceso a la red; del acceso a las aplicaciones por parte de los usuarios; del control; del itinerario de las operaciones; del itinerario de las tareas; y de los resguardos. Así, se va adquiriendo nuevo conocimiento de cada elemento para hacer una representación e implantación de éstos, mediante reglas; y

finalmente, hacer la validación, mediante pruebas para actualizar las características de cada elemento identificado para las bitácoras.

Posteriormente, se sigue con la planificación de contingencias. Se identifican las características del comité de respuesta a emergencias; del plan de recuperación de desastres; de los acuerdos de operación alterna; y de los adiestramientos y simulacros. Así, se va adquiriendo nuevo conocimiento de cada elemento para hacer una representación e implantación de éstos, mediante reglas; y finalmente, hacer la validación, mediante pruebas para actualizar las características de cada elemento identificado para la planificación de contingencias.

Finalmente, se avanza con la seguridad. Se identifican las características del plan de seguridad; de la arquitectura de seguridad; de las políticas y procedimientos; de los fundamentos; de las bitácoras; y de las medidas de control de seguridad. Así, se va adquiriendo nuevo conocimiento de cada elemento para hacer una representación e implantación de éstos, mediante reglas; y finalmente, hacer la validación, mediante pruebas para actualizar las características de cada elemento identificado para la seguridad.

Al obtener todo este conocimiento, solo atribuible a un experto en el área de seguridad de los sistemas tecnológicos, es que se conforma la confianza en el sistema experto. Permitiendo así, cumplir con el objetivo de que los sistemas expertos son una solución viable para eliminar las vulnerabilidades y riesgos en los sistemas de información de las organizaciones. Refiérase a la Figura 10.

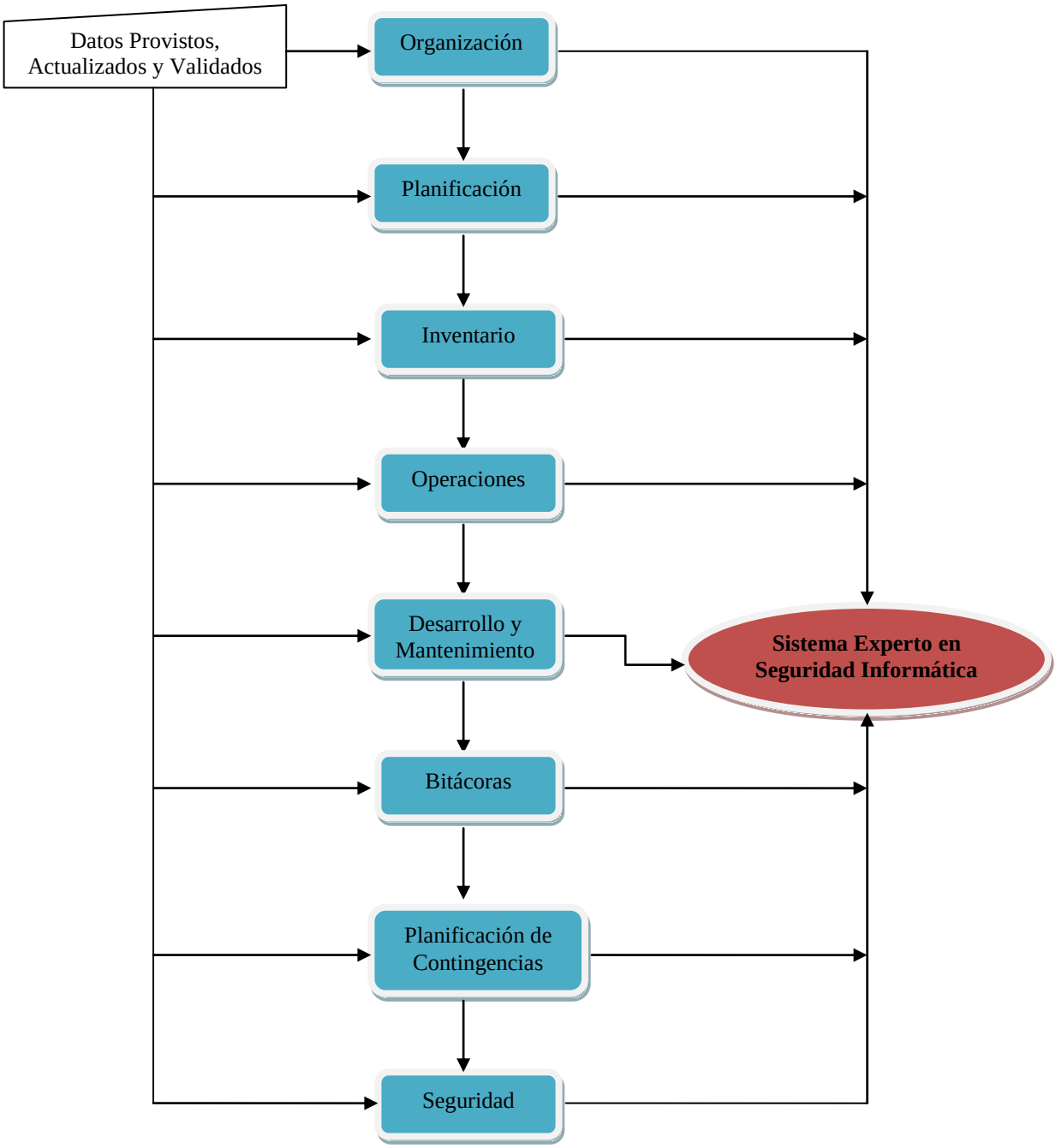

Figura 10. **Proceso de Insumo de Conocimiento para el Sistema Experto en Seguridad Informática**

CONCLUSIONES

Del estudio realizado se desprende que las vulnerabilidades y riesgos en los sistemas de información de las organizaciones pueden ser identificables y prevenibles, si se tiene claramente definido cuáles son los activos informáticos de la organización

(Cintrón, s.f.). Mediante la hoja de cotejo incluida en la Tabla 3, se puede establecer las medidas necesarias para evitarlos; tanto a nivel físico como de programación. En el caso de los sistemas expertos, se requiere establecer unas características—análisis del problema; crear conceptos, estrategias y tareas—adquisición y conceptualización; establecer objetivos, procedimientos reglas—representación e implantación; y hacer la validación—verificación y pruebas, según indican Alty y Coombs (1984).

La literatura indica que los sistemas expertos están siendo utilizados en la industria, el gobierno y otros tipos de instituciones. Muchas organizaciones han desarrollado sistemas expertos para ayudar a una amplia variedad de áreas (Liebowitz, 1990; Sviokla, 1990). Estos hechos por sí solos proporcionan una fuerte evidencia de que la tecnología de los sistemas expertos; en general, ha sido aplicada con éxito.

Varios estudios de casos han informado de implantaciones exitosas de sistemas expertos en el área financiera— tales como: ExperTAX y Authorizer's Assistant de American Express— y los importantes beneficios de estos sistemas (O'Neal y Palese, 1988; Shpilberg et al., 1986). Además, de establecer cómo la tecnología de los sistemas expertos ha ganado credibilidad y su aplicación en las organizaciones, se ha convertido en una poderosa herramienta de negocios para uso personal y para que las organizaciones obtengan una ventaja competitiva (Feigenbaum, McCorduck y Nii, 1988; Liebowitz, 1990). Por otra parte, como la inversión en la tecnología crece, también crece la necesidad de evaluar más detenidamente la recuperación de la inversión y para entender mejor los factores relacionados con el éxito o el fracaso en la utilización de la tecnología.

La aplicación de los sistemas expertos será adecuada donde los expertos dispongan de conocimientos complejos en un área estrechamente delimitada, donde no existan algoritmos elaborados— o donde los existentes no puedan solucionar algún

problema— y no existan teorías completas. Otro ámbito de su aplicación es donde hay teorías, pero resulta prácticamente imposible analizar todos los casos teóricamente imaginables mediante algoritmos y en un espacio de tiempo razonable. En estas situaciones hace falta el conocimiento que el experto ha adquirido por experiencia, para llegar a una solución en un espacio de tiempo aceptable.

Además, los dos tipos de problemas descritos se caracterizan por el hecho de que, aunque es posible la existencia de una o más soluciones, la vía de soluciones no está previamente fijada. Sin embargo, el experto encuentra una solución al problema gracias a la información que posee del problema y a su experiencia. Mientras esta solución sea idónea de repetición y el planteamiento del problema sea claro, existe un razonamiento que puede ser reproducido por un sistema experto.

Finalmente, se puede concluir de esta investigación que debido a que la estructuración y la implantación del conocimiento del experto requieren una gran cantidad de trabajo, solo valdrá la pena el esfuerzo de crear un sistema experto cuando pueda constatarse que el conocimiento particular sea válido durante un largo periodo de tiempo y vaya a ser utilizado por el mayor número posible de personas. En otros escenarios, el esfuerzo y recursos a invertir no resultan rentables.

RECOMENDACIONES

Se recomienda a quien esté interesado en continuar este tipo de estudio, incluir una mayor cantidad de tipos de sistemas de información— como los sistemas de procesamiento de transacciones, sistemas de apoyo de decisiones y sistemas de información ejecutiva— para comparar su desempeño con relación a la rapidez y precisión con que solucionan la situación o problema asignado. De esta forma se lograría validar o no los resultados obtenidos en esta investigación.

También, se sugiere incluir en otros estudios cómo y en qué medida los factores identificados que contribuyen a las vulnerabilidades y los riesgos de los sistemas informáticos de las organizaciones y, compararlos con los esfuerzos requeridos para erradicarlos. Tales como:

- los factores tecnológicos;
- los factores humanos; y
- los factores organizacionales.

Finalmente, al determinar cuáles son los pasos "costo-efectivos" a seguir se justificaría establecer procedimientos aplicables para la eliminación de las vulnerabilidades y riesgos en las redes y estaciones de trabajo de las organizaciones.

REFERENCIAS

Abraham, R.H. (1990). *A Visual Introduction to Dynamical Systems Theory for Psychology*. Aerial.

Adams, J. (1995). Risk. London, UK: UCL Press.

Acosta, N., Buitrago, R., Newball, M., Ramírez, M.A. & Sánchez, J. (2004). *Análisis de Vulnerabilidades*. Introducción a la Computación Forense – 2004-I. Universidad de los Andes.

Alty, J.L. & Coombs, M.J. (1984). *Expert Systems: Concepts and Examples*. Chichester, Sussex: John Wiley.

Audestad, J. (2005). Four reasons why 100% security cannot be achieved. *Telektronikk, 1*, 38-47.

Barsanti, J.B. (1990). Expert Systems: Critical Success Factors for Their Implementation. *Information Executive, 3, 1*, 30-34.

Beznosov, K. & Beznosova, O. (2007). On the imbalance of the security problem space and its expected consequences. *Information Management & Computer Security, 15, 5*, 420-431.

Botta, D., Werlinger, R., Gagne´, A., Beznosov, K., Iverson, L., Fels, S. & Fisher, B. (2007). *Towards understanding IT security professionals and their tools*. Proceedings of the Symposium on Usable Privacy and Security (SOUPS), 100-111. Pittsburgh, PA: ACM Press.

Bradbury, J. (1989). The policy implications of differing concepts of risk. *Science, Technology, and Human Values, 14, 4*, 380-399.

Byrd, T.A. (1992). Implementation and Use of Expert Systems in Organizations: Perceptions of Knowledge Engineers. *Journal of Management Information Systems, 8, 4*, 97-116.

Chang, S.E. & Ho, C.B. (2006). Organizational factors to the effectiveness of implementing information security management. *Industrial Management & Data Systems, 106*, 345-61.

Cintrón, C.R. (s.f.). *Hoja de cotejo para revisión seguridad de los Activos informáticos*. Material que formó parte del curso GSI 732 - Seguridad de los Recursos de Información del Programa Graduado de Auditoría de Sistemas de Información de la Universidad del Sagrado Corazón.

Cintrón, C.R. (2006). *Implantación de programas de seguridad*. Unidad que formó parte del curso GSI 732 - Seguridad de los Recursos de Información del Programa

Graduado de Auditoría de Sistemas de Información de la Universidad del Sagrado Corazón.

Cross, F.B. (1992). The risk of reliance on perceived risk. *Risk, 3*, 59-70.

Davis, R. (1984). *Amplifying Expertise with Expert Systems*. The AI Business. Cambridge, MA: MIT Press, 17-40.

Dewdney, A.K. (1997). *Yes, We Have No Neutrons: An Eye-Opening Tour through the Twists and Turns of Bad Science*. Hoboken, NJ: Wiley.

Diario Digital Aeronoticias (29 de diciembre de 2009). *¿Qué pasará en el 2010 en materia de seguridad informática?* Extraído el 8 de agosto de 2010 de la página http://www.aeronoticias.com.pe/noticiero/index.php?option=com_content &view=article&id=8308:ique-pasara-en-el-2010-en-materia-de-seguridad-infor matica&catid=27:27&Itemid=136.

Duda, R.O. & Shortliffe, E.H. (1983). Expert System Research. *Science, 220, 4594*, 261-268.

Evans, D. & Paul, N. (2004). Election security: perception and reality. *IEEE Security & Privacy, 2, 1*, 24-31.

Feigenbaum, E., McCorduck, P. & Nii, P. (1988). *The Rise of the Expert Company*. Alexandria, VA: Time Life.

Finkelstein, C. (1989). *An Introduction to Information Engineering: From Strategic Planning to Information Systems*. Sydney: Addison-Wesley.

Firebaugh, M.W. (1989). *Artificial Intelligence: A Knowledge-Based Approach*. Boston, MA: PWS-Kent Publishing Company.

Garigue, R. & Stefaniu, M. (2003). Information security governance reporting. *EDPACS, 31, 6*, 11-17.

Giarratano, J.C. & Riley, G. (2005). *Expert Systems, Principles and Programming*. Boston, MA: PWS Publishing Company.

Gill, T.G. (1995). Early expert systems: where are they now? *MIS Quarterly, 19, 1*, 51-81.

Glock, H.J. (2008). *What Is Analytic Philosophy*. Cambridge, MA: Cambridge University Press.

Goebel, R., Poole, D.L., & Mackworth, A.K. (1997). *Computational intelligence: A logical approach*. Oxford, UK: Oxford University Press.

Haugeland, J. (1985). *Artificial Intelligence: The Very Idea*. Cambridge, MA: MIT Press.

Hauttech Group Ltda. (2010). *Prevención de Intrusión y Evaluación de Infraestructura de Seguridad*. Extraído el 27 de septiembre de 2010 de la página http://www.hauttech.com/servicios2.html#INTRODUCCION

Ignizio, J.P. (1991). *Introduction to Expert Systems*. New York, NY: McGraw-Hill, Inc.

Jasanoff, S. (1998). The political science of risk perception. *Reliability Engineering and System Safety, 59,* 91-99.

Jih, W.J.K. (1990, May). Comparing Knowledge-Based and Transaction Processing Systems Development. *Journal of Systems Management, 21, 5*, 23-28.

Jiwnani, K. & Zelkowitz, M. (2002). Maintaining software with a security perspective. *Proceedings of the International Conference on Software Maintenance*, 194-203.

Kahneman, D. & Tversky, A. (2000). *Choice, Values, Frames*. Cambridge, MA: Cambridge University Press.

Kankanhalli, A., Teo, H., Tan, B.C. & Wei, K. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management, 23*.

Keyes, J. (1989). Why Expert Systems Fail. *AI Expert, 4, 11*, 50-53.

Knapp, K.J., Marshall, T.E., Rainer, R.K. & Ford, F.N. (2006). Information security: management's effect on culture and policy. *Information Management & Computer Security, 14, 1*, 24-36.

Koskosas, I.V. & Paul, R.J. (2004). The interrelationship and effect of culture and risk communication in setting internet banking security goals. *Proceedings of the 6th International Conference on Electronic Commerce*, 341-350. New York, NY: ACM Press.

Kraemer, S. & Carayon, P. (2007). Human errors and violations in computer and information security: the viewpoint of network administrators and security specialists. *Applied Ergonomics, 38,* 143-154.

Laird, J., Rosenbloom, P. & Newell, A. (1987). SOAR: An Architecture for General Intelligence. *Artificial Intelligence, 33,* 1-64.

Lakoff, G. & Johnson, M. (1999). *Philosophy In The Flesh: The Embodied Mind and Its Challenge to Western Thought*. California, USA: Berkeley University Press.

Liebowitz, J. (1990). *Expert Systems for Business & Management*. Englewood Cliffs, New Jersey: Yourdan Press.

Lu, M., & Guimaraes, T. (1988). A Guide to Selecting Expert Systems Applications. *Systems Development Management, 32, 3,* 1-11. Reprinted in Journal of Information Systems Management (1989, Spring), 8-15. Reprinted in Expert Systems (1989, Summer).

Luger, G. (1994). *Cognitive science : the science of intelligent systems*. San Diego, CA: Academic Press.

Luhmann, N. (1995). Social Systems. Stanford, CA: Stanford University Press.

Marcus, G.F. (2001). *The Algebraic Mind: Integrating Connectionism and Cognitive Science (Learning, Development, and Conceptual Change)*. Cambridge, MA: MIT Press.

Nikander, P. & Karvonen, K. (2001). Users and trust in cyberspace, in Christianson, B., Crispo, B., Malcolm, J.A. and Roe, M. (Eds). *Security Protocols: 8th International Workshop, Cambridge, UK, April 3-5, 2000*, revised papers in Vol. 2133, 24-35. Lecture Notes in Computer Science. New York, NY: Springer.

Nilsson, N. (1998). *Artificial Intelligence: A New Synthesis*. Morgan Kaufmann Publishers.

Nunes, M. & Annansingh, F. (2002). The risk factor. *The Journal of the Institute for the Management of Information Systems, 12, 6*, 10-12.

O'Neal, Q. (1990). *Planning and Managing Successful Applications*, presented at IAKE 1990.

O'Neal, Q. & Palese, D. (1988). Developing and Implementing Diagnostic Expert Systems. *IBM Manufacturing Technology Digest, 6, 1*, 43-48.

Pieters, W. (2006). Acceptance of voting technology: between confidence and trust. *Trust Management: 4th International Conference, iTrust 2006, Lecture Notes in Computer Science, 3986*, 283-297. New York, NY: Springer.

Pinker, S. & Mehler, J. (1988). *Connections and Symbols*. Cambridge MA: MIT Press.

Prerau, D.S. (1990). *Developing and Managing Expert Systems*. Reading, MA: Addison-Wesley.

Puig, T. (2008). *Capítulo 7: Identificación de vulnerabilidades e impactos*. Forma parte de un curso a distancia de Gestión de riesgos de los sistemas de información. Extraído el 27 de septiembre de 2010 de la página http://www.mailxmail.com/curso-gestion-riesgos-sistemas-informacion/identificacion-vulnerabilidades-impactos

Pursell, C. (1979). Belling the cat: a critique of technology assessment. *Lex en Scientia, 10*, 130-142.

Puyosa Piña, H.D. (s.f.). *Vulnerabilidad de los Sistemas de Control a ataques informáticos*. Reunión Técnica de ISA Sección Española, Madrid y Cartagena.

Riedl, R. (2004). Rethinking trust and confidence in European e-government: linking the public sector with post-modern society. *Proceedings of the Fourth IFIP Conference on e-Commerce, e-Business, and e-Government (I3E 2004).*

Russell, S.J. & Norvig, P. (2003). *Artificial Intelligence: A Modern Approach* (2nd Ed.). NJ: Prentice Hall: Upper Saddle River.

Shpilberg, D., Graham, L.E. & Schatz, H. (1986). ExperTAX: An Expert System for Corporate Tax Planning. *Expert Systems, 3, 3,* 136-150.

Shrader Frechette, K.S. (1990). Perceived risks versus actual risks: managing hazards through negotiation. *Risk, 1,* 341-363.

Smith, A. (2004). E-security issues and policy development in an information-sharing and networked environment. *New Information Perspectives, 56, 5,* 272-285.

Smith, D.L. (1988, December). Implementing Real World Expert Systems. *AI Expert, 3, 2,* 51-57.

Straub, D.W. & Welke, R.J. (1998). Coping with systems risk: security planning models for management decision making. *MIS Quarterly, 22, 4,* 441-469.

Strogatz, S. (2007). The End of Insight, in Brockman, John, *What is your dangerous idea?,* Harper Collins.

Sviokla, J. (1990). The Examination of the Impact of Expert Systems on the Firm: The Case of XCON. *MIS Quarterly, 14, 2,* 126-140.

Tsohou, A., Karyda, M. & Kokolakis, S. (2006). Formulating information systems risk management strategies through cultural theory. *Information Management & Computer Security, 14, 3,* 198-217.

Turban, E. (1990). *Decision Support and Export Systems*. New York, NY: MacMillan Publishing Co.

Turban, E., & Watkins, P.R. (1986). Integrating Experts System and Decision Support Systems. *MIS Quarterly, 10, 2,* 121-136.

Tyran, C.K. & George, J.F. (1993, Winter). The Implementation of Expert Systems: A Survey of Successful Implementation. *Data Base,* 5-15.

Xenakis, A. & Macintosh, A. (2005). Procedural security and social acceptance in e-voting. *Proceedings of the 38th Hawaii International Conference on System Sciences (HICSS'05)*.

Websense Inc. (2007). *Riesgos asociados al uso de sistemas de información corporativos*. A

Websense® White Paper. Extraído el 12 de agosto de 2010 de la página http://www.websense.com/assets/white-papers/whitepeper_corp_info_system_risks_es.pdf

Writzel, J.R. & Kerschberg, L. (1989). Developing Knowledge-based Systems: Reorganizing the System Development Life Cycle. *Communications of the ACM, 32, 4*, 482-488.