PROTOTIPO DE SISTEMA EXPERTO PARA LA GENERACIÓN DE NORMAS, POLÍTICAS Y PROCEDIMIENTOS DE SEGURIDAD BASADOS EN LAS NORMAS ISO 17799 E ISO 27001 DENTRO DE UN ENTORNO ORGANIZACIONAL "PSEP"

[*]Juan Jose Bernal Villamarin

[**]Magda Johana Herrera Rada

[***]Roberto Emilio Salas Ruiz

[****]Guillermo Hurtado

Resumen

Con el avance de la tecnología y la gran dependencia generada por los negocios ha surgido, una gran cantidad de amenazas de seguridad procedentes de diferentes fuentes, que explotan al máximo las vulnerabilidades de los sistemas de información y redes de las compañías poniendo en peligro su activo más importante que es la información.

Es por tal motivo que ha surgido este proyecto, PSEP es un Sistema Experto para la gestión de la seguridad de la información que permite generar recomendaciones y políticas que contribuyan a la protección de la información.

PSEP hace una recolección de los procesos que se ejecutan en la organización que tengan relación con la operatividad y continuidad del negocio, la seguridad del personal, controles de acceso físicos y lógicos, desarrollo y mantenimiento de sistemas, gestión de comunicaciones, seguridad física y

[*] Tecnólogo en sistematización de datos de la Universidad Distrital "Francisco José de Caldas". – Facultad Tecnológica. Correo electrónico: beastbernal@hotmail.com.

[**] Tecnóloga en sistematización de datos de la Universidad Distrital "Francisco José de Caldas" – Facultad Tecnológica. Correo electrónico: magdolica @hotmail.com

[***] Ingeniero de Sistemas de la Universidad del Norte, Magíster en Ingeniería de Sistemas de la Universidad Nacional de Colombia. Profesor Universidad Distrital "Francisco José de Caldas" – Facultad Tecnológica. Correo electrónico: resalasr@udistrital.edu.co.

[****] Ingeniero de Sistemas, Especialista en telemática y Magíster en planeación estrategica. Profesor Universidad Distrital "Francisco José de Caldas" – Facultad Tecnológica. Correo electrónico: ghurtado@udistrital.edu.co

ambiental y la clasificación y el control de activos, por medio de cuestionarios referentes a cada modulo.

Por ultimo PSEP toma esta información y la valida con los procedimientos de inferencia y la base de conocimiento que ha sido alimentada con la experiencia de los expertos y genera recomendaciones o políticas de acuerdo a los datos ingresados.

Abstract

With the advance of the technology and the great dependency generated by the businesses has arisen, a great amount of threats of security coming from different sources that vulnerabilities of the network and information systems explode to the maximum of the companies putting in danger their more important assets that is the information.

It is by such reason that has arisen this project; PSEP is an Expert system for the management of the security information that allows to generate recommendations and policies that contribute to the protection of the information.

PSEP will make a harvesting of the processes that are executed in the organization which they have relation with the operability and continuity of the business, the security of the personnel, physical and logical controls access, development and maintenance of systems, management of communications, physical and environmental security and the classification and the control of assets, by means of referring questionnaires to each I modulate

Palabras claves

Sistema Experto, Encadenamiento hacia delante, UML, RUP, Tabla Hash, Colección MAP, Seguridad.

Keywords

Expert System, forward chaining, UML RUP, Hhash table, MAP Collection, Security.

Introducción

Un experto se puede considerar como una persona que es especialista en un área determinada, ahora un sistema hace referencia a un conjunto de conceptos estructurados y organizados, si se unen estas dos definiciones tendremos la base de un sistema experto.

Este es el concepto en el cual se basa el proyecto, donde se desarrollo una herramienta que permite a las personas encargadas de la seguridad de la información de la organización, facilitarle la implementación de las políticas de seguridad, basados en las experiencias de los expertos en los diferentes campos de la tecnología informática, que reunieron sus conocimientos en las normas ISO 17799 e ISO 27001.

La herramienta se centra en orientar al encargado de la seguridad de la información en indicarle que debe hacer para desarrollar la gestión de la seguridad de la información de acuerdo a lo descrito en las normas.

1. Generalidades

1.1. Sistemas Expertos

Sistemas Expertos se entiende un tipo de software que imita el comportamiento de un experto humano en la solución de un problema.

Pueden almacenar conocimientos de expertos para un campo determinado y solucionar un problema mediante deducción lógica de conclusiones.

La función de un Sistema Experto es la de aportar soluciones a problemas, como si de humanos se tratara, es decir, capaz de mostrar soluciones inteligentes. Y ¿Cómo es posible?, es posible gracias a que el sistema es creado con información de expertos (humanos), que intentan estructurar y formalizar conocimientos poniéndolos a disposición del sistema, para que este pueda resolver una función dentro del ámbito del problema, de igual forma que lo hubiera hecho un experto.

Como esquema para el desarrollo de la herramienta PSEP se utilizaron los sistemas de producción, que es el esquema más comúnmente empleado en sistemas Expertos, utiliza reglas para la representación del conocimiento. Un sistema de producción consta de:

- Una porción de memoria que se utiliza para rastrear el estado actual del universo bajo consideración.
- Un conjunto de reglas de producción
- Un interpretador que examine el estado actual y ejecute las reglas de producción aplicables

Como estrategia de razonamiento, existen dos métodos generales de inferencia que se usan en los sistemas expertos, que son: encadenamiento hacia adelante y encadenamiento hacia atrás.

El encadenamiento hacia adelante es el razonamiento desde los hechos hacia las conclusiones que resultan de ellos; el encadenamiento hacia atrás implica el razonamiento en reversa desde la hipótesis, habrá de comprobarse una posible conclusión a los hechos que la sustentan.

1.2. Norma ISO 17799 – 21007:2005

ISO 17799 es una norma internacional que ofrece recomendaciones para realizar la gestión de la seguridad de la información dirigida a los responsables de iniciar, implantar o mantener la seguridad de una organización, define la información como un activo que posee valor para la organización y requiere por tanto de una protección adecuada. El objetivo de la seguridad de la información es proteger adecuadamente este activo para asegurar la continuidad del negocio, minimizar los daños a la organización y maximizar el retorno de las inversiones y las oportunidades de negocio.

La seguridad de la información se define como la preservación de:

• **Confidencialidad:** Aseguramiento de que la información es accesible sólo para aquellos autorizados a tener acceso.
• **Integridad:** Garantía de la exactitud y completitud de la información y de los métodos de su procesamiento.
• **Disponibilidad:** Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados.

El objetivo de la norma ISO 17799 es proporcionar una base común para desarrollar normas de seguridad dentro de las organizaciones y ser una práctica eficaz de la gestión de la seguridad.

ISO 17799 está organizada en 10 secciones:

- Políticas de seguridad - Esto proporciona a la alta dirección el apoyo para la seguridad de la información.
- Organización de activos y recursos - para ayudarle a administrar la seguridad de la información dentro de la organización.
- Clasificación y control de activos - para ayudarle a identificar sus activos y protegerlos apropiadamente.
- Seguridad del personal - para reducir los riesgos de error humano, robo, fraude o mal uso de las instalaciones y equipo.
- Seguridad ambiental y física - para prevenir acceso sin autorización, daños e interferencia a las instalaciones del negocio y a la información.
- Comunicaciones y administración de operaciones - para asegurar la operación correcta y segura de las instalaciones de procesamiento de la información.
- Control de acceso - para controlar el acceso a la información.
- Sistemas de desarrollo y mantenimiento - para asegurar que se introduzca la seguridad a los sistemas de información.
- Administración de continuidad del negocio - para contrarrestar las interrupciones a las actividades del negocio y para proteger procesos críticos del negocio contra los efectos causados por fallas mayores o desastres
- Acatamiento - para evitar infracciones a las leyes criminales y civiles, estatutarias, obligaciones regulatorias o contractuales, y cualquier otro requisito de seguridad.

El estándar ISO/IEC 27001 es el nuevo estándar oficial, su título completo en realidad es: BS 7799-2:2005 (ISO/IEC 27001:2005) También fue preparado por el comité JTC 1 y en el subcomité SC 27, IT “Security Techniques”.

La versión que se considerará en este texto es la primera edición, de fecha 15 de octubre de 2005, si bien en febrero de 2006 acaba de salir la versión cuatro del mismo.

Este estándar propone toda una secuencia de acciones tendientes al "establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del ISMS (Information Security Management System)".

Los detalles que conforman el cuerpo de esta norma, se podrían agrupar en tres grandes líneas:

- ISMS.
- Valoración de riegos (Risk Assesment)
- Controles[1].

1.3. Metodología

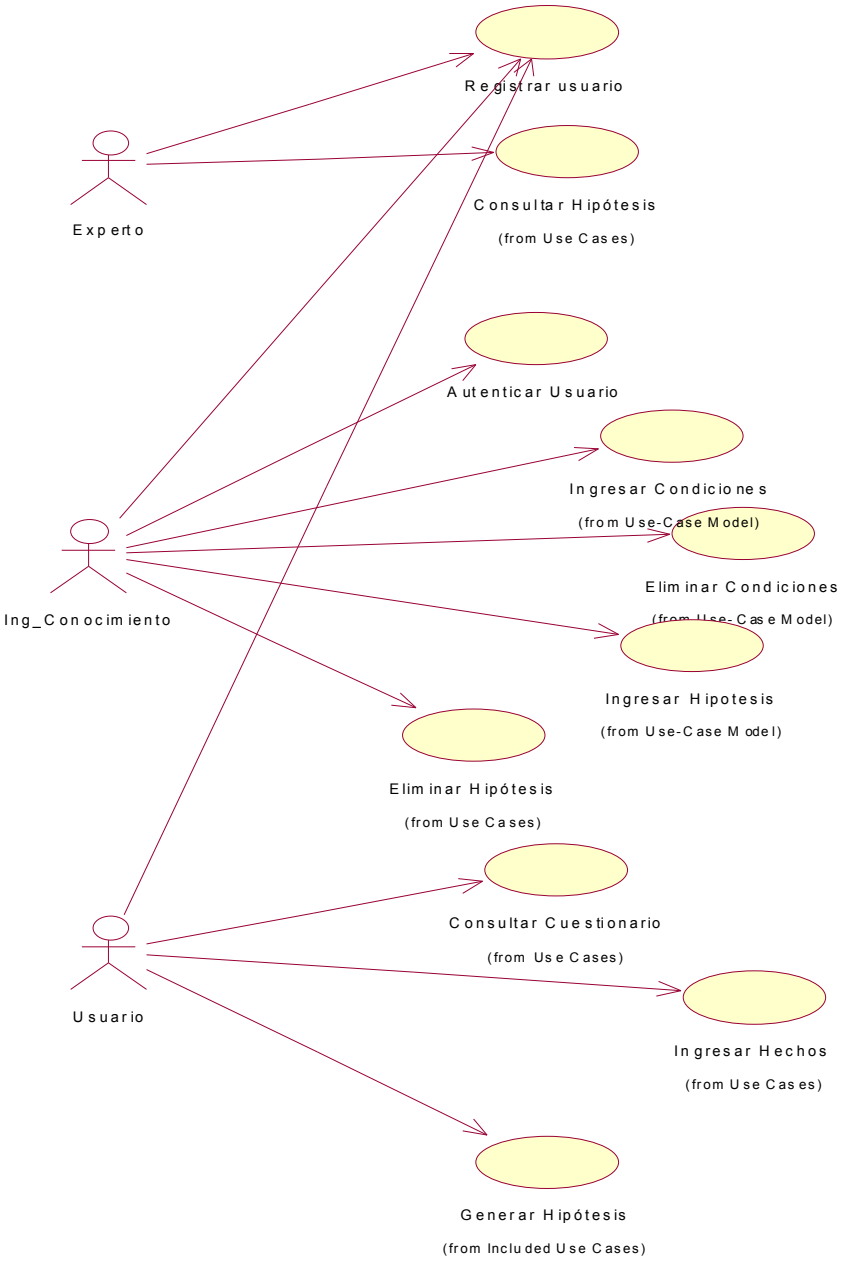
Para la metodología se tomo el RUP[2], es un proceso de desarrollo de software y junto con el UML[3], constituye la metodología estándar más utilizada para el análisis, implementación y documentación de sistemas orientados a objetos.

El RUP divide el proceso de desarrollo en ciclos inicio, elaboración, construcción.

Para el análisis de requerimientos se utilizaron los casos de uso (Figura 1) y los diagramas de modelamiento, en los cuales se describen las acciones realizadas por los actores involucrados en el sistema.

[1] Véase Introducción al análisis de ISO-27001:2005, http://www.desarrolloweb.com/
[2] Racional Unified Process
[3] Lenguaje Unificado de Modelado

Figura 1. Diagrama de Casos de Uso del sistema



1.4. Fase de diseño

Como mecanismo de inferencia se utilizó el encadenamiento hacia delante que es el razonamiento desde los hechos hacia las conclusiones que resultan de ellos.

Para dar la solución se utilizó el razonamiento guiado por los datos porque el mecanismo de inferencia usa información proporcionada por el usuario para moverse a través de las reglas e inferir las consecuencias que se derivan de ella.

Para el sistema PSEP se seleccionó este método puesto que se parte de unos hechos para generar nuevos hechos.

Adicionalmente, se utilizó la estructura básica de las tablas hash y la colección MAP[4] de java para llevar a cabo el desarrollo. El siguiente esquema demuestra el funcionamiento que tendrá:

Grupo 1

1 ¿Existe un proceso de autorización para nuevas instalaciones de procesamiento en el cual se involucre los sistemas de información?

2 ¿Al momento de adquirir hardware o software se analiza que sea compatible con los demás componentes del sistema?

Suponiendo que el usuario contesta positivamente a las dos condiciones, entonces se crea un arreglo de la siguiente forma:

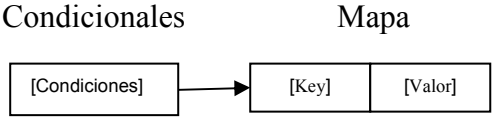
[Si,Si] y se compara con la Tabla 1 de recomendaciones que tiene la siguiente estructura:

[4] Un Map (correspondencia) es un objeto que asocia una clave a un valor. También se denomina Diccionario.

Tabla 1. Esquema general de las recomendaciones.

Grupo 1	
[Si,Si]	[Las nuevas instalaciones deben llevar la autorización de los responsables del proceso. realizando con anterioridad la prueba de compatibilidad de hardware y software con los componentes del sistema. adicionalmente si se va a hacer uso de medios de procesamiento personales para procesar información de negocio o cualquier utilización del medio deben ser valorados y autorizados.]
[Si,No]	[Se recomienda adicionalmente a la autorización para nuevas instalaciones realiza la prueba de compatibilidad de hardware y software para determinar que son compatibles con los demás componentes del sistema]
[No,No]	[Se recomienda adicionalmente a la autorización para nuevas instalaciones realizar la prueba de compatibilidad de hardware y software para determinar que son compatibles con los demás componentes del sistema y valorar y autorizar los medios de procesamiento de información personal]
[No,Si]	[Se recomienda documentar y establecer un procedimiento claro acerca de los procesos de autorización para nuevas instalaciones de procesamiento que involucren software y hardware de la compañía]

Al momento de encontrar la combinación adecuada se asigna el valor, en este caso seria la hipótesis que se encuentra en le primer lugar. El diagrama general sería de la forma:



1.5. Herramienta de desarrollo

Como herramienta de desarrollo se utilizó Java, el cual es un lenguaje de programación Orientado a Objetos, con el que podemos realizar cualquier tipo de programa independiente de la plataforma, puesto que cuenta con una maquina virtual para cada sistema operativo que hace de puente. Para el diseño se utilizó Macromedia Flash.

2. Herramienta PSEP

Como resultado de todo este análisis y diseño se obtuvo un sistema modular con el objeto de facilitar el uso por parte del encargado de la seguridad de la información y la administración dada por el ingeniero del conocimiento.

La seguridad esta dada por los roles que asigne el ingeniero del conocimiento desde le módulo de administración, lo que hace que las bases del conocimiento estén protegidas y se tenga control y veracidad sobre la información ingresada.

En su entorno de Usuario, cuenta con tres módulos que son: Definiciones, Procedimiento y Aplicación

En el módulo de Definiciones se encuentran los conceptos básicos de la seguridad informática, en los Procedimientos se encuentran algunas prácticas que es recomendable revise antes de iniciar la generación de políticas de seguridad.

En la opción de Aplicación encuentran 5 módulos, se puede iniciar desde cualquiera de estos.

Figura 2. Módulos PSEP

Cada modulo cuenta con un cuestionario, el cual pretende que el usuario diligencie las opciones de acuerdo a los procedimientos de la organización (ver figura 3)..

Figura 3. Cuestionarios PSEP

Y tomando como referencia esta información el sistema genere las políticas o recomendaciones según sea, después de realizar la inferencia de los datos con la base de conocimiento (Figura 4).

Figura 4. Recomendaciones PSEP

Cabe resaltar que la precisión de las recomendaciones o políticas dependen de la información ingresada por el usuario.

En el módulo de administrador se tiene que se ingresan grupos de condiciones con diferentes opciones y cada grupo genera una hipótesis, el formato general es de la forma mostrada en la figura 5.

Figura 5. Módulo de administrador

3. Resultados.

El sistema PSEP fue probado dentro de una importante empresa multinacional que lleva 8 años en el mercado y cuenta con una tecnología robusta.

Los resultados arrojados por PSEP detectaron fallas como vicios del sistema, vulnerabilidades, falta de controles internos y externos, en algunas áreas restringidas no se contaba con los controles mínimos, entre otros.

Las políticas que generó fueron acordes a las que ya estaban establecidas lo que amplio la confiabilidad del sistema PSEP.

Los comentarios de las personas que utilizaron el sistema fueron que es muy fácil y agradable a la vista como punto positivo y como oportunidad de mejora que es un poco extenso y tiene algunas preguntas complejas.

4. Perspectivas.

PSEP se utilizará como una herramienta que generará recomendaciones y aspectos a mejorar a la infraestructura, además de una serie de políticas y procedimientos que aplicarán a una organización contribuyendo a realizar prácticas eficaces de la gestión de la información dentro de la organización teniendo en cuenta las reglamentaciones que aplican en el campo.

Se espera que PSEP se actualice periódicamente con los cambios que surgen en cuanto a procedimientos en el campo de la seguridad de la información.

5. Conclusiones.

- El sistema PSEP es una herramienta para los administradores o personas encargadas de la información, puesto que optimiza los tiempos de revisión de los procedimientos de la organización respecto a las normas ISO 17799 e ISO 27001

- Con el sistema PSEP se reduce significativamente el tiempo que toma el proceso de planeación e implementación para generar las políticas de seguridad de la información

- Como forma de representación del conocimiento se utiliza el sistema de producción, el cual es una de las formas más usuales para la implementación de sistemas expertos ya que proporciona una estructura que facilita la descripción y la ejecución de un proceso de búsqueda utilizando las reglas de producción que simulan el pensamiento humano.

- En la base de conocimiento del sistema PSEP, se han reunido los conocimientos de varios expertos Administradores de red los cuales participaron en la elaboración de la norma

- El sistema PSEP le recomienda las mejores prácticas al encargado de la seguridad de la información acorde con lo estipulado en la norma

Referencias bibliográficas

[1] DERRIEN Y. Técnicas de la Auditoría Informática: La dirección de la misión de la auditoria, México D.F., 1995.

[2] ROLSTON, D. W. Principios de Inteligencia Artificial y Sistemas Expertos. California: McGraw Hill, 1990.

[3] BOOCH, G.; RUMBAUGH, J. y JACOBSON, I. El lenguaje unificado de modelado. Madrid, España : Addison Wesley, 2000.

[4] BOOCH, G.; RUMBAUGH, J. y JACOBSON, I. Análisis y diseño orientado a objetos con aplicaciones. Addison-Wesley: Diaz de Santos,1995

[5] BOOCH, G.; RUMBAUGH, J. y JACOBSON, I. El lenguaje unificado de modelado – Manual de referencia. Madrid, España : Addison Wesley, 2000.

[6] GIARRATANO, Joseph y GARY, Riley. Sistema Experto principios y programación, Berkeley: Internacional Thomson Editores, 2001.

[7] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN, NTC-ISO/IEC 17799 Código de buenas practicas para la gestión de la seguridad de la información, ICONTEC, Bogota, 2004.