MÉTRICAS DE SEGURIDAD EN LOS SGSIs, PARA CONOCER EL NIVEL DE SEGURIDAD DE LOS SS.OO Y DE LOS SGBD

L. E. Sánchez[1], A.Santos-Olmo[2], E. Fernández-Medina[3], M. Piattini[4], Grupo de Investigación Alarcos/GsyA, Universidad de Castilla-la Mancha (Ciudad Real, España)

Recibido Noviembre 16, 2011 – Aceptado Marzo 1, 2012
http://dx.doi.org/10.18566/puente.v6n1.a04

***Resumen*— La sociedad de la información cada vez depende más de los Sistemas de Gestión de la Seguridad de la Información (SGSI), y poder disponer de estos sistemas ha llegado a ser vital para la evolución de las PYMES. Sin embargo, este tipo de compañías requiere de SGSIs adaptados a sus especiales características, y que estén optimizados desde el punto de vista de los recursos necesarios para implantarlos y mantenerlos. Este artículo se centra en el desarrollo de un proceso para SGSIs que permita conocer el nivel de seguridad de las aplicaciones críticas instaladas en estos sistemas, es decir, sistemas operativos y sistemas de Gestión de Bases de Datos. Este modelo está siendo aplicado directamente a casos reales, consiguiendo así una constante mejora en su aplicación.**

***Palabras clave*— Asociatividad academia y empresa, Desarrollo Tecnológico, Innovación, competitividad Departamental.**

***Abstract*— The information society is ever-increasingly dependent upon Information Security Management Systems (ISMSs), and the availability of these systems has come to be vital to the evolution of SMEs. However, this type of companies requires ISMSs which have been adapted to their particular characteristics, and which are optimized from the point of view of the resources that are necessary to install and maintain them. This paper concentrates on the development of a process for ISMSs that will allow the level of security of critical applications installed in these systems, i.e., Operative Systems and Data Base Management Systems, to be measured. This process is currently being directly applied in real cases, thus leading to an improvement in its application.**

***Keywords*— Industry-Academy Associativity, Technological Development, Innovation, State Competitivity,**

[1] L. E. Sánchez, Sicaman Nuevas Tecnologías, Tomelloso (Ciudad Real), España, lesanchez@sicaman-nt.com
[2] A. Santos-Olmo, Sicaman Nuevas Tecnologías, Tomelloso (Ciudad Real), España, asolmo@sicaman-nt.com
[3] E. Fernandez-Medina, Universidad de Castilla-la Mancha, Ciudad Real, España, Eduardo.FdezMedina@uclm.es
[4] M. Piattini, Universidad de Castilla-la Mancha, Ciudad Real, España, Mario.Piattini@uclm.es

I. INTRODUCCIÓN

Para las empresas, es muy importante implantar controles de seguridad que les permitan conocer y controlar los riesgos a los que pueden están sometidas [1, 2], ya que la implantación de estos controles supone obtener importantes mejoras para estas compañías [3]. Pero la implantación de estos controles no es suficiente, siendo necesaria la presencia de sistemas que gestionen la seguridad a lo largo del tiempo, de modo que les permita reaccionar ágilmente ante nuevos riesgos, vulnerabilidades, amenazas, etc. [4, 5]. Sin embargo, es frecuente que las empresas no tengan sistemas de gestión de la seguridad, o que si los tienen, estos estén elaborados sin unas guías adecuadas, sin documentación y con recursos insuficientes [6]. Además, la mayor parte de las herramientas de seguridad disponibles en el mercado ayudan a solucionar parte de los problemas de seguridad, pero son pocas las que abordan el problema de la gestión de la seguridad de una manera global e integrada. De hecho, la enorme diversidad de estas herramientas y su falta de integración suponen un enorme coste en recursos para poderlas gestionar.

Por lo tanto, a pesar de que la realidad ha demostrado que para que las empresas puedan utilizar las tecnologías de la información y las comunicaciones con garantías es necesario disponer de guías, métricas y herramientas que les permitan conocer en cada momento su nivel de seguridad y las vulnerabilidades que aún no han sido cubiertas [7], el nivel de implantación con éxito de estos sistemas realmente es muy bajo. Este problema se acentúa especialmente en el caso de las pequeñas y medianas empresas, que cuentan con la limitación adicional de no tener recursos humanos y económicos suficientes para realizar una adecuada gestión [6].

De acuerdo a investigaciones recientes [8], el éxito de los SGSI depende principalmente de los siguientes factores: i) enfocar la seguridad hacia el negocio; ii) implementar la seguridad en consonancia con la cultura de la empresa; iii) conseguir el apoyo indiscutible, visible y comprometido de la dirección de la empresa; iv) conseguir entender bien los requisitos de seguridad, de la evaluación y gestión de los riesgos; v) concienciar tanto a directivos como a empleados de la necesidad de la seguridad; vi) ofrecer formación y guías sobre políticas y normas a toda la organización; vii) definir un sistema de medición para evaluar el rendimiento de la gestión de la seguridad y sugerir mejoras. Para el caso de las PYMEs, estos factores son importantes, pero además, el SGSI debe estar optimizado en cuanto a recursos necesarios, y también debe tener un alcance suficiente, para no descuidar la seguridad, pero no excesivo, para controlar su coste. Por ese motivo, es muy importante poder contar con metodologías para la gestión de la seguridad de la información que estén especialmente diseñadas para este tipo de empresas, y que además permitan reutilizar el conocimiento y la experiencia previamente adquiridos, de modo que su implantación sea más rápida, más certera y más económica.

En este artículo nos centramos en analizar un método orientado a cumplir el séptimo de estos factores -"definir un sistema de medición para evaluar el rendimiento de la gestión de la seguridad y sugerir mejoras"-, adaptándolo al caso de las PYMES para conseguir que su coste de mantenimiento sea muy reducido, ofreciendo al responsable de seguridad el máximo valor posible, permitiéndole conocer cómo evoluciona el nivel de cumplimiento de los diferentes controles en el corto plazo.

El artículo continúa en la Sección 2, describiendo brevemente los objetivos que se han perseguido a lo largo de la investigación. En la Sección 3 se describe el proceso de medición utilizado. En la Sección 4 se analizan los objetivos de control elaborados para la fase actual de la investigación. En la Sección 5, se presenta la herramienta que da soporte al proceso definido. En la Sección 6, se muestran algunos de los resultados obtenidos durante la aplicación del proceso en una empresa. Finalmente, en la Sección 7 concluimos indicando cuál será el trabajo que desarrollaremos en el futuro.

II. OBJETIVO PERSEGUIDO CON LA INVESTIGACIÓN

Desarticulación A partir de esta visión de la situación actual del mercado y de las necesidades de seguridad de las empresas, se ha centrado el objetivo de esta investigación en elaborar un proceso que permita medir de una forma sencilla, pero eficiente, el nivel de seguridad de aquéllas aplicaciones que podemos considerar críticas para el correcto funcionamiento del Sistema de Información de una compañía, así como una herramienta que dé soporte a este proceso y ofrezca la posibilidad de automatizar parte de las pruebas a efectuar en el sistema y obtener un informe final con el estado de securización de sus principales aplicaciones de trabajo. Este proceso permitirá obtener una garantía del riesgo que se asume con el Sistema Informático de una empresa, con un menor coste tanto en tiempo como económico, lo que la hace de gran utilidad para las PYMES.

A la hora de elaborar estas métricas, se han tenido en cuenta las últimas investigaciones realizadas sobre los estándares más importantes relacionados con las métricas de seguridad [9, 10]. El mecanismo elaborado no pretende sustituir a estas normas, sino complementarlas y ayudar a su cumplimiento.

Los ámbitos en los que se ha centrado el análisis de los objetivos de control iniciales del proceso son:

- Sistemas Operativos: Debe verificarse en primer lugar que los Sistemas Operativos están actualizados con las últimas versiones y actualizaciones del fabricante. El análisis de las versiones de los Sistemas Operativos permite descubrir las posibles incompatibilidades entre otros productos de Software Básico adquiridos por la instalación y determinadas versiones de aquéllos.

- Sistemas de Gestión de Base de Datos: El diseño de las Bases de Datos se ha convertido en una actividad muy compleja y sofisticada. El proceso analizará los Sistemas de salvaguarda de datos existentes, revisará la integridad de los mismos y la consistencia de los datos almacenados, así como la ausencia de redundancias entre ellos.

Por lo tanto, podemos definir que el principal objetivo de la investigación ha sido crear un proceso que permita definir una serie de aspectos medibles y

valorables sobre aplicaciones críticas y una herramienta que lo soporte, la cual permita ofrecer una valoración objetiva y un informe del riesgo actual de los Sistemas Operativos y de los Sistemas de Gestión de Bases de datos, elementos clave de los Sistemas de Información de una compañía, con los que se integran y sobre los que se sustenta el resto de aplicaciones corporativas. Este proceso se integrará con el resto de procesos que forman parte de un SGSI.

El alcance de la fase actual de la investigación se ha limitado a: a) Desarrollar todos los objetivos de control a nivel de Sistema Operativo y SGBD; b) Desarrollar una herramienta que dé soporte al proceso y permita realizar la revisión del nivel de cumplimiento de seguridad en base a los objetivos de control definidos; c) Analizar qué objetivos de control pueden ser automatizados en el SGBD; y d) Su validación en los entornos de desarrollo y producción de una compañía de desarrollo de Software.

Para alcanzar el objetivo propuesto en la investigación, se han seguido cuatro fases claramente diferenciadas:

1. *Fase 1*. Durante la 1ª fase se ha analizado cómo definir un sistema sencillo que nos permita valorar el nivel de seguridad actual de las aplicaciones críticas.

2. *Fase 2*. Durante la 2ª fase se han extraído de las herramientas seleccionadas para la investigación cuales serían los principales factores a valorar para definir su nivel de seguridad. Se ha procedido a realizar un estudio en profundidad del S.O. Windows y de los dos SGBD más utilizados actualmente (Oracle y SQL Server), definiendo los objetivos de control que permitan realizar posteriormente una valoración del nivel de seguridad, así como el sistema de valoración que se utilizará para la securización del entorno.

3. *Fase 3*. Durante la 3ª fase se ha creado una aplicación que permitirá servir de soporte a la realización de los análisis sobre el proceso definido en la fase 1ª. Como resultado se ofrecerá una valoración del grado de securización de los sistemas analizados según su configuración actual. También se obtendrán unas recomendaciones asociadas a las acciones a acometer para aumentar el nivel de seguridad de los Sistemas de Información. Dicha aplicación estará formada por cuatro partes: a) Entrada de parámetros para el análisis; b) Rellenado manual de una parte del checklist; c) Escaneo y rellenado automático de una parte del checklist; y d) Emisión del informe.

4. *Fase 4*. Por último, en la 4ª fase, se aplicará el proceso y la herramienta que lo soporta sobre diversos sistemas que funcionan en la compañía. Con este proceso se obtendrá un conjunto de resultados que permitirán determinar el nivel de securización actual de los sistemas de esta empresa, así como recomendaciones sobre cómo mejorarlo.

III. DESARROLLO DEL PROCESO DE MEDICIÓN

La Para el desarrollo de esta fase se realizó una selección previa de aquellas herramientas y aplicaciones que ante un fallo de seguridad pudieran tener un mayor impacto en los servicios informáticos de una compañía. Los resultados de este estudio demuestran que el mayor riesgo asumido por una empresa es la pérdida o filtración no deseada de sus datos.

En base a los resultados de este análisis se llegó a la conclusión de que las aplicaciones críticas en cualquier sistema informático que funcione bajo una plataforma Microsoft son el S.O. y los sistemas de soporte a datos, por lo que se seleccionaron para el desarrollo del proyecto las siguientes aplicaciones: Sistemas Operativos Windows y Sistemas de Gestión de Bases de Datos Oracle y SQL Server.

El siguiente paso de esta fase fue determinar para cada una de esas aplicaciones cuáles eran sus objetivos de control, así como determinar unas pruebas y niveles que permitieran evaluar el nivel de riesgo actual del sistema.

Para desarrollar dichos objetivos de control se contó con la documentación técnica sobre seguridad ofrecida por las compañías fabricantes, así como con la experiencia personal del equipo humano participante. En base a este conocimiento, se seleccionaron para cada aplicación aquellos puntos que suponían mayor riesgo. Posteriormente cada uno de estos puntos se discretizó para poder cuantificarlo.

El mecanismo de cuantificación o valoración de los objetivos de control está basado únicamente en el

conocimiento de las aplicaciones ofrecidos por los expertos, lo cual implica que pueden sufrir variaciones en versiones posteriores de la investigación.

La estructura que se ha seguido para definir los objetivos de control ha sido:

- Id: Código único que permite identificar el objetivo de control y la aplicación a la que pertenece.
- Nivel: En el entorno global, a qué nivel afecta el objetivo de control.
- Pregunta: Objetivo de control perseguido.
- Responsabilidad: Quién es el responsable de aplicar dicho objetivo de control
- Instante: Determina en qué instante debería haberse testeado el objetivo de control.
- Acción: Determina la forma en que verificar el objetivo de control.
- Configuración correcta: Cómo debería estar el objetivo de control para considerase seguro.
- Valoración: Criterios para decidir si se cumple o no el objetivo de control, estableciendo si el mismo es seguro o inseguro.

Como conclusión a la ejecución del proceso definido, se obtendrá un nivel de securización de la aplicación, que será calculado como se muestra en la TABLA I.

TABLA I.
FÓRMULAS PARA CALCULAR EL NIVEL DE CUMPLIMIENTO DE UN CONTROL

NR = (([PTVE]*100)/[PTVP])   ***NS = 100 – NR***
• *NR: Nivel de riesgo.*   • *NS: Nivel de securización.*   • *PTVE: Puntuación total de las vulnerabilidades encontradas.*   • *PTVP: Puntuación total de las vulnerabilidades posibles.*

Según el valor obtenido tendremos el riesgo asociado, discretizado en la TABLA II:

TABLA II
NIVELES DE MEDICIÓN DEL RIESGO

Riesgo	Intervalo (según el nivel de securización)	Descripción
Sin Riesgo	90% - 100%	No se han detectado fallos graves.
Riesgo potencial	60% - 90%	Se han detectado fallos de nivel medio.
Alto riesgo	0% - 60%	Se han detectado fallos de nivel alto.

IV. DEFINICIÓN DE LOS CONTROLES

En esta fase de la investigación, se han analizado en detalle un conjunto de aplicaciones críticas, con el objetivo de extraer el conjunto de objetivos de control para cada una de las aplicaciones que han formado parte de la investigación. Las aplicaciones analizadas han sido:

– Windows Server: Se ha extraído un conjunto de 25 controles a valorar. El total de puntos que definirá el nivel de securización de la aplicación varía de 0 (máximo nivel de securización) a 37 (mínimo nivel de securización). En la TABLA III se puede ver un ejemplo de control definido para este tipo de aplicaciones. Los aspectos a valorar se encuentras divididos en 5 tipologías: i) Nivel de acceso: Incluye 8 aspectos valorables que afectan a los accesos del sistema; ii) Nivel de servicio: Incluye 8 aspectos que afectan a los servicios del sistema, y a los usuarios con acceso a ellos; iii) Nivel de aplicaciones: Incluye 3 aspectos que afectan a la seguridad de las aplicaciones instaladas en el sistema; iv) Nivel de gestión: Incluye ocho aspectos que afectan a la gestión y administración del sistema y v) Nivel de red: Incluye 2 aspectos que afectan a la configuración de red, así como vulnerabilidades sensibles de ser explotadas desde el exterior.

TABLA III.
CONTROL MANUAL PARA WINDOWS SERVER

Id: [W2K.4.6]
Pregunta: ¿Existe copia de seguridad de los contenidos del Registro?
Nivel: Gestión.
Responsabilidad: Administrador.
Instante: Operativa.
Acción: Registro.
Configuración correcta: Mantener una copia de seguridad actualizada del Registro.
Valoración:
- ***Inseguro:*** No existe una copia del registro, o ésta no se realiza periódicamente.
- ***Seguro***: Existe una copia de seguridad actualizada del registro, y esta se realiza periódicamente en periodos definidos.

– SQL Server: Se ha extraído un conjunto de 37 controles sobre los que valorar el nivel de cobertura de seguridad, de los cuales 26 pueden ser automatizados para reducir costes y 13

requieren actualmente de un análisis manual. El total de puntos que definirá el nivel de securización de la aplicación varia de 0 (máximo nivel de securización) a 53 (mínimo nivel de securización). En la TABLA 4 se puede ver un ejemplo de los controles definidos para este tipo de aplicaciones. Los aspectos a valorar se encuentran divididos en 4 tipologías: i) Nivel general: Incluye 4 aspectos valorables que afectan directamente al entorno de la máquina, sobre la que se encuentra implantado el SGBD; ii) Nivel servidor: Incluye 3 aspectos valorables que afectan directamente a la configuración del servidor, sobre el que se encuentra implantado el SGBD; iii) Nivel SGBD: Incluye 26 aspectos valorables que afectan directamente al Sistema de Gestión de Base de Datos; y iv) Nivel BD: Incluye 4 aspectos valorables que afectan directamente a las Bases de Datos.

– Oracle: Se ha extraído un conjunto de 26 controles sobre los que se debe valorar el nivel de cobertura de seguridad. El total de puntos que definirá el nivel de seguridad de la aplicación varia de 0 (máximo nivel de securización) a 44 (mínimo nivel de securización). En la TABLA 5 se puede ver un ejemplo de control definido para este tipo de aplicaciones. Los aspectos a valorar se encuentras divididos en 4 tipologías: i) Nivel general: Incluye 6 aspectos valorables que afectan al entorno de la maquina sobre la que se encuentra instalado el SGBD, ii) Nivel servidor: Incluye 5 aspectos valorables que afectan directamente a la configuración del servidor, sobre el que se encuentra instalado el SGBD; iii) Nivel SGBD: Incluye 10 aspectos valorables que afectan directamente al Sistema de Gestión de Base de Datos; y iv) Nivel BD: Incluye 5 aspectos valorables que afectan directamente a las Bases de Datos.

TABLA IV
CONTROL MANUAL/AUTOMÁTICO PARA SQL SERVER

Id: [SQL.4.2]
Pregunta: ¿Se utilizan vistas para minimizar las dependencias entre BD?
Nivel: Base de Datos.
Responsabilidad: Programador.
Instante: General.
Acción: Control de código.
Configuración correcta: Proteger contra el acceso vía SQL mediante el desarrollo de una programación estructurada.

TABLA IV
CONTROL MANUAL/AUTOMÁTICO PARA SQL SERVER (Continuación)

Valoración:
- ***Inseguro:*** Existen dependencias entre BD que no están contenidas en vistas.
- ***Seguro:*** Se utilizan vistas para minimizar las dependencias entre BD.

Prueba solicitada: Analizar las dependencias con servidores vinculados y verificar el tipo de objetos que las contienen. Usar para ellos las tablas sysservers, sysobjects, syscomments.

Script para automatización:

```
select srvname collate SQL_Latin1_General_CP1_CI_AS
from master.dbo.sysservers
declare @servidor varchar(128)
select @servidor = ''
select total, servidor_novista, servidor_vista,
case when total=0 then 0 else
100*convert(decimal(9,2),servidor_novista)/convert(decim
al(9,2),total) end as porc_servidor_novista,
 case when total=0 then 0 else
100*convert(decimal(9,2),servidor_vista)/convert(decimal
(9,2),total) end as porc_servidor_vista
   from (select count(*) as total,
         isnull(sum(case when xtype='V' then 1 else 0
end),0) servidor_vista,
         isnull(sum(case when xtype='V' then 0 else 1
end),0) servidor_novista
       from sysobjects a, syscomments b
where text like '%'+@servidor+'%') a
```

TABLA V
CONTROL MANUAL/AUTOMÁTICA PARA ORACLE

Id: [ORA.4.3]
Pregunta: ¿Se ha realizado la optimización del área de Shared Pool?
Nivel: Base de Datos.
Responsabilidad: Administrador del sistema.
Instante: Creación y mantenimiento de aplicaciones. Podemos englobarla dentro de una acción de "Cuenta de Servicios".
Acción: Cuenta de Servicios.
Configuración correcta: Garantizar el uso de la zona de memoria para obtener un buen rendimiento en las aplicaciones Oracle en la máquina.
Valoración:
- *Inseguro:* Si el tamaño de esta estructura es pequeño se empezarán a producir contenciones dentro del sistema, bajando el rendimiento y tiempos de respuesta.
- *Seguro:* El tamaño se ajusta a las necesidades de las aplicaciones.

Prueba solicitada: Se revisarán el área de almacenamiento compartido de sentencias SQL (library cache) y el área de almacenamiento del diccionario de datos (dictionary cache): En la primera consulta, si el ratio obtenido es menor que 95%, indica que se está produciendo paginación y habría que aumentar el valor del parámetro SHARED_POOL_SIZE de INIT.ORA. Si el ratio de la segunda consulta es mayor al 1%, indica que se están produciendo excesivos fallos en library cache..

TABLA V
CONTROL MANUAL/AUTOMÁTICA PARA ORACLE
(Continuación)

En la última sentencia, el RATIO obtenido deberá tener una tasa de aciertos cercana al 90%, ya que si no se estarían produciendo excesivos fallos en los accesos Script para automatización: *Select (sum(pins-reloads))/sum(pins) * 100 "RATIO" From v$librarycache; Select sum(pins) "NUMERO DE EJECUCIONES", sum(reloads) "NUMERO DE FALLOS EN MEMORIA", sum (reloads)/(sum(pins)+sum(reloads))*100 "RATIO" From v$librarycache; Select (1-(sum(getmisses)/(sum(gets)+sum(getmisses))))*100 "RATIO" From v$rowcache;*

V. HERRAMIENTA

Se ha realizado una herramienta que dé soporte automatizado al proceso desarrollado y que pueda integrarse dentro de la herramienta global para SGSI denominada MGSM-TOOL [15]. Esta herramienta, permite iniciar la auditoría (ver Fig. 1), introduciendo unos parámetros de configuración iniciales: a) Nombre de la computadora (Dominio\nombre): nombre de la maquina sobre la que se quiere realizar la auditoría; b) Dirección IP: Dirección de la maquina a auditar; c) Nombre del informe: nombre con el que se guardará el informe de auditoría, para poderlo consultar posteriormente; d) Aplicaciones a analizar: en esta versión la auditorías son excluyentes, es decir, para realizar una auditoría de SQL Server y Windows Server sobre el mismo servidor deberán realizarse 2 auditorías diferentes; e) Login y password: permitirá establecer la cadena de conexión en la BD para lanzar los scripts; y f) Base de datos: Base de datos dentro de un SGBD sobre la que se quiere realizar una auditoría más detallada.

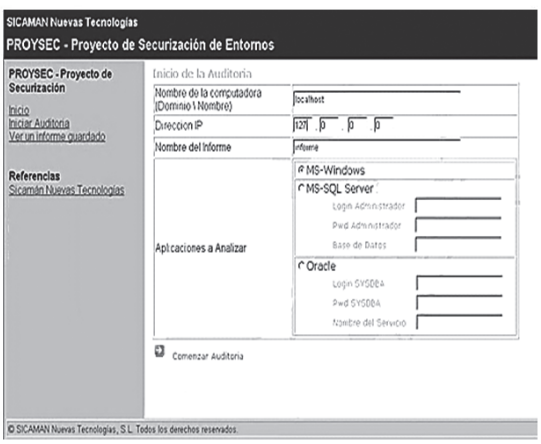

Fig. 1. Pantalla de inicio de la aplicación

Al pulsar sobre la opción "Realizar Auditoría", nos iremos a los objetivos de control que conformar la auditoría (ver Fig. 2).

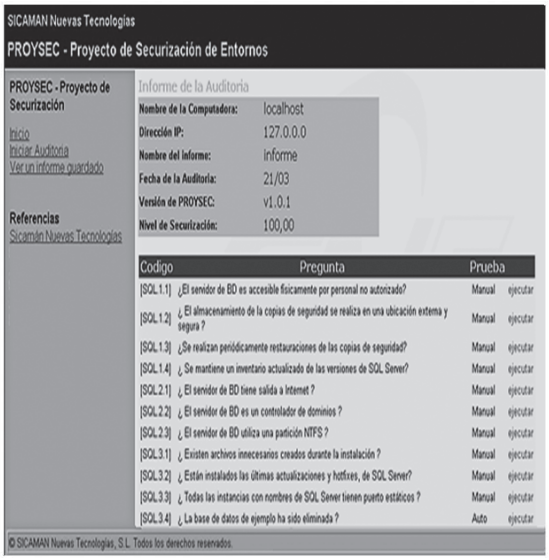

Fig. 2. Controles para determinar el nivel de seguridad.

Pulsando sobre la opción de ejecutar de un objetivo de control, podremos consultar toda la información disponible para ese objetivo de control (ver Fig. 3) y almacenar el resultado del análisis. En caso de que el objetivo de control sea automático, al ejecutar se cargará el resultado y el grado asignado, y el Auditor podrá modificarlo o complementarlo.

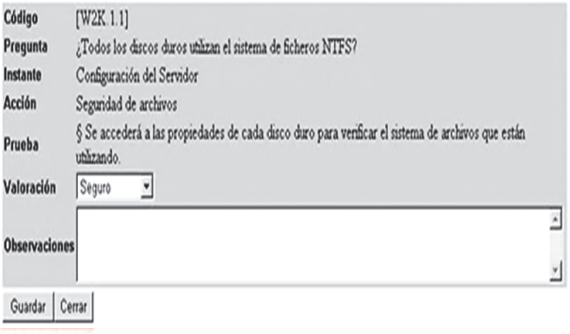

Fig. 3. Ficha de control

En el caso de que los objetivos de control estén automatizados ellos emitirán una lista de observaciones y una valoración de forma automática y el auditor podrá modificarla si no está de acuerdo con ella.

La aplicación desarrollada, también permite acceder a un histórico de las auditorías realizadas con anterioridad para comparar la evolución (ver Fig. 4).

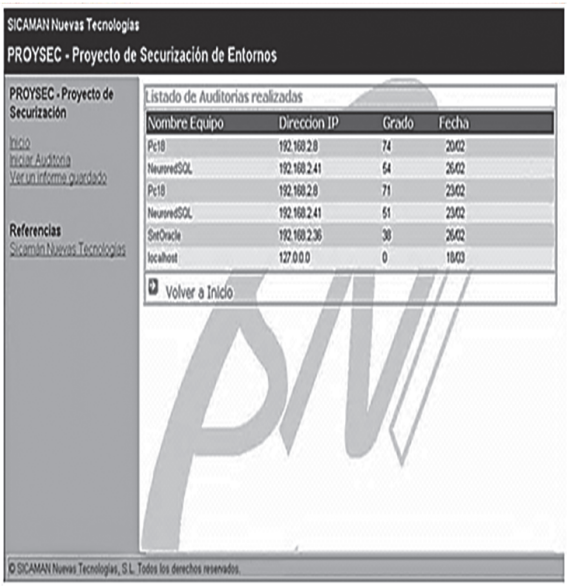

Fig. 4. Pantalla de auditorías realizadas

Al pulsar sobre una auditoría obtendremos el resultado de los objetivos de control de la misma (ver Fig. 5).

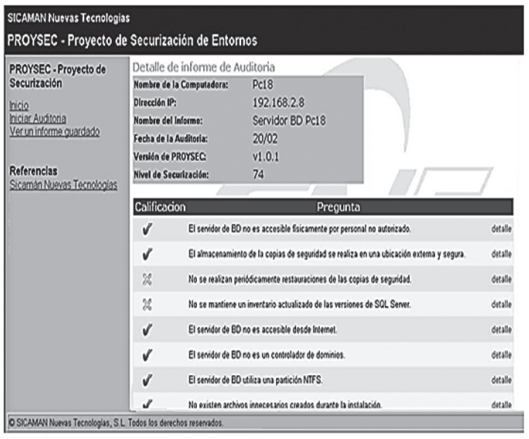

Fig. 5. Resultado auditoria

Si pinchamos sobre el detalle de un objetivo de control obtendremos en detalle, la prueba que se realizó y las observaciones que se realizaron sobre la misma (ver Fig. 6).

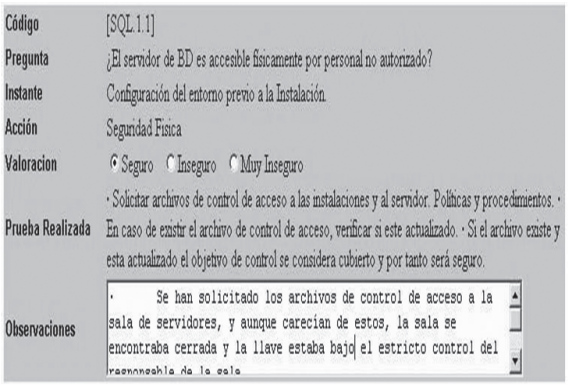

Fig. 6. Ficha de resultados a nivel de control

De esta forma el sistema permite medir de una forma rápida el nivel de seguridad de un conjunto de aplicaciones críticas, instaladas en nuestro sistema.

VI. RESULTADOS PRÁCTICOS

Las pruebas del sistema se han realizado sobre las instalaciones de la compañía Sicaman (SNT), en servidores de desarrollo y producción, sobre sistemas operativos Windows Server 2003 y Sistemas de Gestión de Bases de Datos Oracle 11i y SQL Server 2005. En la TABLA VI. se pueden ver algunas de las conclusiones obtenidas al aplicar el proceso definido sobre aplicaciones reales.

Como conclusión de la aplicación del método definido sobre los entornos de desarrollo y producción de SNT se obtuvieron los siguientes resultados:

- El servidor de producción para el entorno SQL Server 2005, ha obtenido una valoración para la aplicación "Windows 2003 Server" de 10 sobre 37, lo que implica un riesgo potencial del 27,03% y un nivel de securización del 72,97%
- El servidor de producción para el entorno SQL Server 2005, ha obtenido una valoración para la aplicación "SQL Server 2005" de 14 sobre 53, lo que implica un riesgo potencial del 26,42% y un nivel de securización del 73,58%
- El servidor de desarrollo para el entorno SQL Server 2005, ha obtenido una valoración para la aplicación "Windows 2003 Server" de 18 sobre 37, lo que implica un riesgo alto del 51,35% y un nivel de securización del 48,65%

- El servidor de desarrollo para el entorno SQL Server 2005, ha obtenido una valoración para la aplicación "SQL Server 2005" de 25 sobre 53, lo que implica un riesgo alto del 47,17% y un nivel de securización del 52,83%
- El servidor de desarrollo para el entorno Oracle 11i, ha obtenido una valoración para la aplicación "Windows 2003 Server" de 18 sobre 37, lo que implica un riesgo alto del 51,35% y un nivel de securización del 48,65%
- El servidor de desarrollo para el entorno Oracle 11i, ha obtenido una valoración para la aplicación "Oracle 11i" de 21 sobre 44, lo que implica un riesgo alto del 47,73% y un nivel de securización del 52,27%.

Las conclusiones finales obtenidas son:

- El entorno de producción de SNT tiene un nivel de securización medio, tanto a nivel de servidor, como a nivel de aplicaciones individuales. Sería aconsejable seguir las recomendaciones obtenidas durante la ejecución del proceso, sobre todo teniendo en cuenta que es un entorno de producción.
- El entorno de desarrollo de SNT tiene un nivel de securización bajo, tanto a nivel de servidor, como a nivel de aplicaciones individuales, tanto para entornos SQL Server como para entornos Oracle. Lo aconsejable para un entorno de desarrollo es situar el riesgo en un nivel medio, por lo que se aconseja seguir las recomendaciones del informe de auditoría.

TABLA VI
RESULTADOS DE LA APLICACIÓN DE LAS MÉTRICAS EN CASOS REALES

Datos Sistemas	Resultados obtenidos
Nombre del ordenador: Sicaman\NeuroredSQL **Dirección IP:** 192.168.2.41 **Nombre del Equipo a Auditar:** Servidor BD NeuroredSQL **Fecha de la Auditoría:** 24/11/2010 10:15 **Escaneado con la versión de SEM:** 1.0 **Nivel de Securización:** 18/37 → 51,35% **Nivel de Riesgo:** 48,65% (Alto riesgo).	La puntuación negativa ha sido de 18 sobre 37 lo cual implica que el nivel de securización actual de la plataforma auditada es de 51,35% con un riesgo asociado del 58,65%. Para aumentar el nivel de securización deberán revisarse los siguientes puntos: ***Riesgo muy alto:*** [W2K.2.3], [W2K.2.4], [W2K.5.2] ***Riesgo alto:*** [W2K.1.2], [W2K.1.3], [W2K.1.5], [W2K.1.8], [W2K.2.1], [W2K.2.2], [W2K.3.1], [W2K.3.3] , [W2K.4.2], [W2K.4.3], [W2K.4.4], [W2K.4.6]

TABLA VI
RESULTADOS DE LA APLICACIÓN DE LAS MÉTRICAS EN CASOS REALES (Continuación)

Datos Sistemas	Resultados Obtenidos
Nombre del ordenador: Sicaman\Pc18 **Dirección IP:** 192.168.2.8 **Nombre del Equipo a Auditar:** Servidor BD **Fecha de la Auditoría:** 20/11/2010 9:46 **Escaneado con la versión de SEM:** 1.0 **Nivel de Securización:** 14/53 → 73,58% **Nivel de Riesgo:** 26,42% (Riesgo Potenc)	La puntuación negativa ha sido de 14 sobre 53 lo cual implica que el nivel de securización actual de la plataforma auditada es de 73,58% con un riesgo asociado del 26,42%. Para aumentar el nivel de securización deberán revisarse los siguientes puntos: ***Riesgo muy alto:*** [SQL.3.2], [SQL.3.10], [SQL.3.25] ***Riesgo alto:*** [SQL.1.3], [SQL.1.4], [SQL.3.3], [SQL.3.7], [SQL.3.9], [SQL.3.22], [SQL.3.24], [SQL.4.4]
Nombre del ordenador: Desarrollo\SNTOracle **Dirección IP:** 192.168.2.36 **Nombre del Equipo a Auditar:** SntOracle **Fecha de la Auditoría:** 26/11/2010 18:20 **Escaneado con la versión de SEM:** 1.0 **Nivel de Securización:** 21/44 → 52,27% **Nivel de Riesgo:** 47,73% (Alto riesgo).	La puntuación negativa ha sido de 21 sobre 44 lo cual implica que el nivel de securización actual de la plataforma auditada es de 52,27% con un riesgo asociado del 47,73%. Para aumentar el nivel de securización deberán revisarse los siguientes puntos: ***Riesgo muy alto:*** [ORA.1.1], [ORA.1.2], [ORA.1.3], [ORA.2.4], [ORA.3.1], [ORA.3.4], [ORA.3.5], [ORA.3.10] , [ORA.2.1] ***Riesgo alto:*** [ORA.1.4], [ORA.1.5], [ORA.1.6]

El nivel de riesgo obtenido en las revisiones se puede ver en la TABLA VII y el nivel de cobertura de seguridad actual para las aplicaciones analizadas se puede ver en la TABLA VII.

TABLA VII
NIVEL DE RIESGO PARA LAS APLICACIONES ANALIZADAS

	Windows 2003	SQL 2005	Oracle 11i	Riesgo medio
Servidor desarrollo [SQL]	48,65	47,17	-	47,78
Servidor desarrollo [ORA]	48,65	-	47,73	48,15
Servidor producción [SQL]	27,03	26,42	-	26,67

TABLA VIII
NIVEL DE COBERTURA DE SEGURIDAD PARA LAS APLICACIONES ANALIZADAS

	Windows 2003	SQL 2005	Oracle 11i	Securizac media
Servidor desarrollo [SQL]	51,35	52,83	-	52,22
Servidor desarrollo [ORA]	51,35	-	52,27	51,85
Servidor producción [SQL]	72,97	73,58	-	73,33

Las conclusiones finales obtenidas son:

- El entorno de producción de SNT tiene un nivel de securización medio, tanto a nivel de servidor, como a nivel de aplicaciones individuales. Sería aconsejable seguir las recomendaciones obtenidas durante la ejecución del proceso, sobre todo teniendo en cuenta que es un entorno de producción.
- El entorno de desarrollo de SNT tiene un nivel de securización bajo, tanto a nivel de servidor, como a nivel de aplicaciones individuales, tanto para entornos SQL Server como para entornos Oracle. Lo aconsejable para un entorno de desarrollo es situar el riesgo en un nivel medio, por lo que se aconseja seguir las recomendaciones del informe de auditoría.

VII. CONCLUSIONES Y TRABAJOS FUTUROS

En este artículo se ha presentado la propuesta de un proceso orientado a medir el nivel de seguridad de aplicaciones críticas que forman parte de un sistema de información.

Se ha definido cómo se puede utilizar este proceso y cómo puede ayudar a que las PYMES conozcan los riesgos a los que se están enfrentando, sin tener que asumir grandes costes.

Las características ofrecidas por el proceso y su orientación a las PYMES ha sido muy bien recibidas, y su aplicación está resultando muy positiva ya que permite que este tipo de empresas entiendan mejor los riesgos a los que están sometidos sus activos de información. Además, con este proceso se obtienen resultados a corto plazo y se reducen los costes que suponen otros mecanismos de análisis, consiguiendo un mayor grado de satisfacción de la empresa.

Actualmente se está analizando la posibilidad de integrar este proceso dentro de la metodología de Gestión de la Seguridad para PYMES denominada MGSM-PYME [11-14], y de la herramienta que da soporte a la metodología [15].

Gracias al desarrollo de este proyecto de investigación, las compañías sobre las que se ha testado han podido identificar riesgos de seguridad y aspectos mejorables en sus sistemas.

En posteriores versiones de la aplicación se continuará con el proceso de automatización de objetivos de control aquí iniciado.

Finalmente, se considera que el trabajo realizado debe ser ampliado con nuevas aplicaciones, nuevos controles, así como mecanismos que permitan incluir cada vez más controles automatizados.

Todas las mejoras futuras del proceso y el modelo se están orientando a mejorar el nivel de automatización y precisión del mismo, pero siempre respetando el principio de coste de recursos, es decir, se busca mejorar el proceso sin incurrir en costes de generación y mantenimiento del mismo.

AGRADECIMIENTOS

Esta investigación es parte de los proyectos MEDUSAS (IDI-20090557) y ORIGIN (IDI-2010043) financiado por el CDTI y el FEDER, BUSINESS (PET2008-0136) concedido por el Ministerio Español de Ciencia y Tecnología y MARISMA (HITO-2010-28), SISTEMAS (PII2I09-0150-3135) y SERENIDAD (PII11-0327-7035) financiado por la Consejería de Educación y Ciencia de la Junta de Comunidades de Castilla-la Mancha.

REFERENCIAS

[1] Kluge, D. Formal Information Security Standards in German Medium Enterprises. in CONISAR: The Conference on Information Systems Applied Research. 2008.
[2] Dhillon, G. and J. Backhouse, Information System Security Management in the New Millennium. Communications of the ACM, 2000. 43(7): p. 125-128.
[3] Park, C.-S., S.-S. Jang, and Y.-T. Park, A Study of Effect of Information Security Management System[ISMS] Certification on Organization Performance. IJCSNS International Journal of Computer Science and Network Security., 2010. 10(3): p. 10-21.

[4] Barlette, Y. and V. Vladislav. Exploring the Suitability of IS Security Management Standards for SMEs. in Hawaii International Conference on System Sciences, Proceedings of the 41st Annual. 2008. Waikoloa, HI, USA.
[5] Fal, A.M., Standardization in information security management Cybernetics and Systems Analysis 2010. 46(3): p. 181-184.
[6] Wiander, T. and J. Holappa, Theoretical Framework of ISO 17799 Compliant. Information Security Management System Using Novel ASD Method., in Technical Report, V.T.R.C.o. Finland, Editor. 2006.
[7] Wiander, T. Implementing the ISO/IEC 17799 standard in practice – experiences on audit phases. in AISC '08: Proceedings of the sixth Australasian conference on Information security. 2008. Wollongong, Australia.
[8] Dojkovski, S., S. Lichtenstein, and M.J. Warren. Challenges in Fostering an Information Security Culture in Australian Small and Medium Sized Enterprises. in 5th European Conference on Information Warfare and Security. 2006. Helsinki, Finland: 1-2 June.
[9] Yao, L., Discussion on Effectiveness Measurement in ISMS: Based on Analysis of ISMS Effectiveness Measurement in ISO/IEC 27004:2009. Electronic Product Reliability and Environmental, 2010.
[10] ISO/IEC27004, ISO/IEC FCD 27004, Information Technology - Security Techniques - Information Security Metrics and Measurement (under development). 2009.
[11] Sánchez, L.E., et al. Security Management in corporative IT systems using maturity models, taking as base ISO/IEC 17799. in International Symposium on Frontiers in Availability, Reliability and Security (FARES'06) in conjunction with ARES. 2006. Viena (Austria).
[12] Sánchez, L.E., et al. MMISS-SME Practical Development: Maturity Model for Information Systems Security Management in SMEs. in 9th International Conference on Enterprise Information Systems (WOSIS'07). 2007b. Funchal, Madeira (Portugal). June.
[13] Sánchez, L.E., et al. Developing a model and a tool to manage the information security in Small and Medium Enterprises. in International Conference on Security and Cryptography (SECRYPT'07). 2007a. Barcelona. Spain.: Junio.
[14] Sánchez, L.E., et al. Developing a maturity model for information system security management within small and medium size enterprises. in 8th International Conference on Enterprise Information Systems (WOSIS'06). 2006. Paphos (Chipre). March.
[15] Sánchez, L.E., et al. SCMM-TOOL: Tool for computer automation of the Information Security Management Systems. in 2nd International conference on Software and Data Technologies (ICSOFT'07). 2007c. Barcelona-España Septiembre.

BIOGRAFÍA

Luis Enrique Sánchez is PhD and MsC in Computer Science and is an Assistant Professor at the Escuela Superior de Informática of the Universidad de Castilla- La Mancha in Ciudad Real (Spain) (Computer Science Department, University of Castilla La Mancha, Ciudad Real, Spain), MSc in Information Systems Audit from the Polytechnic University of Madrid, and Certified Information System Auditor by ISACA. He is the Director of Professional Services and R&D departments of the company Sicaman Nuevas Tecnologías S.L. COIICLM board or committee member and responsible for the professional services committee. His research activities are management security system, security metrics, data mining, data cleaning, and business intelligence. He participates in the GSyA research group of the Department of Computer Science at the University of Castilla- LaMancha, in Ciudad Real (Spain). He belongs to various professional and research associations (COIICLM, ATI, ASIA, ISACA, eSEC, INTECO, etc).

Antonio Santos-Olmo is MsC in in Computer Science and is an Assistant Professor at the Escuela Superior de Informática of the Universidad de Castilla- La Mancha in Ciudad Real (Spain) (Computer Science Department, University of Castilla La Mancha, Ciudad Real, Spain), MSc in Information Systems Audit from the Polytechnic University of Madrid, and Certified Information System Auditor by ISACA. He is the Director of Software Factory departments of the company Sicaman Nuevas Tecnologías S.L. His research activities are management security system, security metrics, data mining, data cleaning, and business intelligence. He participates in the GSyA research group of the Department of Computer Science at the University of Castilla- LaMancha, in Ciudad Real (Spain). He belongs to various professional and research associations (COIICLM, ATI, ASIA, ISACA, eSEC, INTECO, etc).

Eduardo Fernández-Medina holds a PhD. and an MSc. in Computer Science from the University of Sevilla. He is an Associate Professor at the Escuela Superior de Informática of the University of Castilla-La Mancha in Ciudad Real (Spain) (Computer Science Department, University of Castilla La Mancha, Ciudad Real, Spain)- his research activity being in the field of security in information systems, and particularly in security in business processes, databases, datawarehouses, and web services. Fernández-Medina is co-editor of several books and chapter books on these subjects, and has published several dozens of papers in national and international conferences (BPM, UML, ER, ESORICS, TRUSTBUS, etc.). He is author of several manuscripts in national and international journals (Decision Support Systems, Information Systems, ACM Sigmod Record, Information Software Technology, Computers & Security, Computer Standards and Interfaces, etc.). He leads the GSyA research group of the Department of Computer Science at the University of Castilla-La Mancha, in Ciudad Real, Spain and belongs to various professional and research associations (ATI, AEC, AENOR, IFIP WG11.3, etc.).

Mario Piattini is MSc and PhD in Computer Science from the Technical University of Madrid and is a Certified Information System Auditor (CISA) and Certified Information Security Manager by ISACA (Information System Audit and Control Association). He is a professor in the Department of Computer Science at the University of Castilla-La Mancha, in Ciudad Real, Spain. Author of several books and papers on databases, software engineering and information systems, he leads the ALARCOS research group of the Department of Computer Science at the University of Castilla-La Mancha, in Ciudad Real, Spain. He is author of several books and papers on databases, security, software engineering and information systems. He leads the ALARCOS research group of the Department of Computer Science at the University of Castilla- La Mancha, in Ciudad Real (Spain). His research interests are: advanced database design, database quality, software metrics, object-oriented metrics and software maintenance.