VI CONGRESO IBEROAMERICANO DE SEGURIDAD INFORMÁTICA CIBSI 2011

Noviembre 2, 3 y 4

Bucaramanga, Colombia

CIBSI 2011

POLITÉCNICA

Universidad Pontificia Bolivariana
SECCIONAL BUCARAMANGA

20 años 1991 - 2011 UPB BUCARAMANGA

Actas del VI Congreso Iberoamericano de Seguridad Informática
CIBSI 2011
Bucaramanga, Colombia, 2 al 4 de Noviembre de 2011

Editores
Angélica Flórez Abril
Jorge Ramió Aguirre
Arturo Ribagorda Garnacho
Jeimy J. Cano Martínez

ISBN: 978-958-8506-18-0

Facultad de Ingeniería Informática, Universidad Pontificia Bolivariana, Seccional Bucaramanga, Colombia
Universidad Politécnica de Madrid, España

Prefacio

El Congreso Iberoamericano de Seguridad Informática (CIBSI) es una iniciativa de la Red Temática de Criptografía y Seguridad de la Información. Desde el año 2002 se ha venido desarrollando, tomando en cuenta durante los primeros años la realización con frecuencia anual y a partir del año 2003 se realiza cada dos años.

La primera versión del CIBSI fue desarrollada en el año 2002 en Morelia, México; en el año 2003 se celebra la segunda edición en Ciudad de México; en el año 2005 se realizó la tercera edición en Valparaíso, Chile; la cuarta edición tiene lugar en el año 2007 en Mar del Plata, Argentina; y en el año 2009 se celebra la quinta versión en Montevideo, Uruguay.

Éste año 2011, se desarrolla la sexta versión del congreso, teniendo como sede la Universidad Pontificia Bolivariana de Bucaramanga, Colombia, institución educativa que desde el año 2005 se encuentra ofreciendo programas de educación continua en seguridad de la información y a partir del año 2007 ofrece la Especialización en Seguridad Informática, convirtiéndose de ésta manera en una institución que apalanca el desarrollo docente e investigación en seguridad de la información en Colombia.

Para los investigadores del área de seguridad de la información en Colombia, es muy grato realizar por primera vez el CIBSI 2011, evento que facilita el intercambio de conocimiento y la formación de redes de colaboración en el ámbito de la investigación y el desarrollo en seguridad de la información.

Dentro de la agenda programada del evento se tienen definidos tres espacios: conferencias magistrales, ponencias de los trabajos presentados y el Primer Taller Iberoamericano de Enseñanza e Innovación Educativa en Seguridad de la Información (TIBETS).

Se realizarán tres conferencias magistrales por parte de reconocidos investigadores en el área, tales como el Dr. Sergio Rajsbaum de la Universidad Nacional Autónoma de México, el Dr. Justo Carracedo de la Universidad Politécnica de Madrid y el Dr. Jeimy Cano de la Universidad Pontificia Bolivariana de Bucaramanga.

Este documento contiene los trabajos a ser presentados como ponencias por investigadores de diversos países a nivel de Iberoamérica. Se recibieron 39 trabajos, de los cuales el Comité del Programa seleccionó 23 trabajos provenientes de los siguientes países: Argentina, Cuba, Colombia, España, Venezuela, Uruguay, México y Brasil.

Como nuevo aporte, en el marco del CIBSI se realizará el TIBETS, espacio que se dedicará a presentar las experiencias en enseñanza e innovación educativa en el área de seguridad de la información, nuevos rumbos docentes, análisis de proyectos de colaboración conjunta y programas de posgrados, que permita plantear estrategias de colaboración docente.

Se espera que estas actas y las reflexiones realizadas del 2 al 4 de noviembre en el Campus de la Universidad Pontificia Bolivariana de Bucaramanga sirvan para el fortalecimiento de la investigación en seguridad de la información, la generación de nuevos espacios de discusión y el estrechamiento de lazos interinstitucionales para el avance en programas de posgrados y rumbos docentes en el área.

Organización de la Conferencia

Comité Organizador General
Angélica Flórez Abril, Universidad Pontificia Bolivariana, Colombia
Jorge Ramió Aguirre, Universidad Politécnica de Madrid, España

Comité Organizador Logístico

Angélica Flórez Abril, Universidad Pontificia Bolivariana, Colombia
Jeimy Cano Martínez, Universidad Pontificia Bolivariana, Colombia
Reinaldo Mayol Arnao, Universidad Pontificia Bolivariana, Colombia

Comité Técnico

Reinaldo Mayol Arnao, Universidad Pontificia Bolivariana, Colombia
Con el apoyo de los estudiantes de Ingeniería Informática:
Miguel Gerardo Mateus Marín y Julián Eduardo Ramírez Rico

Comité del Programa

Jeimy Cano (Chair)	Universidad Pontificia Bolivariana
Arturo Ribagorda Garnacho (Chair)	Universidad Carlos III de Madrid
Marco Aurélio Amaral Henriques	State University of Campinas - Unicamp
Nicolás Antezana Abarca	Sociedad Peruana de Computación
Javier Areitio Bertolín	Universidad de Deusto
Gustavo Betarte	Universidad de la República
Joan Borrel Viader	Universidad Autónoma de Barcelona
Pino Caballero Gil	Universidad de La Laguna
Adriano Mauro Cansian	Universidad Estadual Paulista
Enrique Daltabuit Godas	Universidad Nacional Autónoma de México
Ángel Martín Delrey	Universidad de Salamanca
Josep Domingo-Ferrer	Universidad Rovera i Virgili
Josep Lluis Ferrer-Gomilla	Universidad de las Islas Baleares
Amparo Fúster-Sabater	Consejo Superior de Investigaciones Científicas
Juan Pedro Hecht	Universidad de Buenos Aires
Luis Hernandez Encinas	Consejo Superior de investigación
Emilio Hernández	Universidad Simón Bolívar
Leobardo Hernández Audelo	Universidad Nacional Autónoma de México
Julio César López	Universidad Estatal de Campinas
Vincenzo Mendillo	Universidad Central de Venezuela
Josep María Miret Biosca	Universidad de Lleida
Gaspar Modelo-Howard	Universidad Tecnológica de Panamá
Raul Monge	Universidad Técnica Federico Santa María
Guillermo Morales-Luna	Centro de Investigación y Estudios Avanzados

	del IPN
Alberto Peinado Domínguez	Universidad de Malaga
Josep Rifà Coma	Universidad Autónoma de Barcelona
Jorge Blasco Alis	Universidad Carlos III de Madrid
Hugo Francisco González Robledo	Universidad Politécnica de San Luis de Potosí
José María de Fuentes García-Romero de Tejada	Universidad Carlos III de Madrid

Tabla de contenido

A Systematic Review of Security Patterns Used to Develop Security Architectures

R. Ortiz, S. Moral Rubio, J. Garzás and E. Fernández Medina

Abstract— **The new technology business models together with the new tendencies in the computer field are forcing to suffer a constant evolution to maintain their competitiveness in markets. This evolution gives place to a continuous remodeling of the architectures of the companies' systems to adapt them to the new needs. All these changes increase these systems' complexity making them more vulnerable. For this reason, computer attacks against organizations are considerably increasing. To avoid this, information security engineers need reliable and validated solutions to face security problems as well as agile solutions to face the new technological necessities in an optimal way. Security patterns are good mechanisms for performing this task because they provide documented, validated and tested solutions to recurring problems. In this paper we carry out a systematic review to know if there exist proposals using security patterns to develop secure systems, in order to detect shortcomings and new necessities in this field.**

Keywords— **systematic review, security patterns, secures architectures, information security, security.**

I. INTRODUCCIÓN

En los últimos años se ha producido un desarrollo tecnológico vertiginoso. La tecnología se encuentra cada vez más presente en la vida cotidiana de las personas: sanidad, educación, banca y finanzas, servicios de emergencia y otras áreas [1]. Los beneficios que aporta la tecnología son muchos y muy importantes. Pero junto a los beneficios, están surgiendo nuevos problemas ligados al desarrollo tecnológico. Uno de los problemas más importantes es la seguridad de los sistemas de información, debido principalmente al aumento de la complejidad de éstos sistemas [2], y a que las organizaciones han abierto sus bases de datos a internet [3]. A consecuencia de esto, los atacantes tienen más posibilidades de encontrar nuevas vulnerabilidades en los sistemas [4, 5], por lo que el número de ataques ha aumentado de manera significativa y los beneficios obtenidos por los atacantes son cada vez mayores [6].

Por lo tanto, la seguridad de la información es una de las principales preocupaciones para las organizaciones. Por ello, es necesario que los ingenieros de sistemas de estas organizaciones incorporen requisitos de seguridad en las arquitecturas tecnológicas de su corporación, atendiendo siempre a las necesidades de negocio, para, por un lado, salvaguardar sus activos, y por otro lado, minimizar el numero de ataques contra sus sistemas y reducir la efectividad de los mismos [7]. Todo esto sin dejar de estar al día en relación a las últimas tecnologías y poder así ofrecer a sus clientes un catalogo novedoso y amplio de productos y servicios.

Para optimizar la tarea de incorporar seguridad en los sistemas existentes de una forma ágil y óptima, es necesario que los ingenieros dispongan de soluciones fiables, validadas y testeadas. Además, teniendo en cuenta que las grandes organizaciones disponen de grupos de trabajo específicos en cada área, es importante también, que los ingenieros dedicados a la seguridad de los sistemas de una organización ofrezcan soluciones homogéneas a problemas similares con el fin de mantener una estrategia de defensa alineada dentro de la corporación.

Los patrones son una buena herramienta para satisfacer las anteriores necesidades, ya que encapsulan el conocimiento y experiencia de expertos sobre un problema recurrente en una determinada disciplina [8]. En otras palabras, un patrón resuelve un problema específico en un contexto determinado y puede ser adaptado a diferentes situaciones [9].

En los últimos años, los patrones han tenido un gran auge en diferentes disciplinas. Los primeros patrones se utilizaron en la construcción civil (edificios) [10], y recientemente la disciplina en la que más se ha investigado ha sido la ingeniería del software [8, 11]. Varios tipos de patrones han sido descritos hasta la fecha, entre ellos se pueden mencionar los patrones de análisis, patrones de diseño, patrones arquitecturales, patrones de seguridad, etc.

Los ingenieros de seguridad de la información pueden, por tanto, usar patrones de seguridad para construir sistemas de información seguros, ya que son una buena herramienta para sistematizar el proceso a la hora de resolver problemas de seguridad recurrentes, aportando guías para la construcción y evaluación de sistemas seguros [12].

En la actualidad se pueden encontrar numerosos trabajos en el ámbito de los patrones de seguridad [13]. Existen estudios que exponen [14, 15], analizan [16, 17], clasifican [18, 19], seleccionan el mejor patrón para un determinado problema [20, 21] , conforman un repositorio de los patrones existentes [9, 22], etc. Sin embargo, en el presente no existe una revisión sistemática enfocada al análisis y diseño de arquitecturas de seguridad en organizaciones reales y complejas utilizando patrones de seguridad. Nosotros entendemos como arquitecturas de seguridad a diseños de sistemas de información completos, estructurados, coordinados y rigurosos

R. Ortiz, Dep. Seguridad de la Información, Grupo BBVA, Madrid, España, r.ortizpl@gmail.com

S. Moral-Rubio, Dep. Seguridad de la Información, Grupo BBVA, Madrid, España, santiago.moral@bbva.com

J. Garzás, Grupo Kybele, Dep de Lenguajes y Sistemas Informáticos II, Universidad Rey Juan Carlos, Madrid, España, javier.garzas@urjc.es

E. Fernández-Medina, Grupo GSyA, Dep. de Sistemas y Tecnologías de la Información, Universidad de Castilla-la Mancha, Ciudad Real, España, Eduardo.FdezMedina@uclm.es

que dan soporte a procesos de negocio con el fin de reducir el riesgo de pérdida de confidencialidad, integridad y disponibilidad cuando los activos de información son gestionados.

La ausencia de este tipo de estudios sobre los patrones de seguridad hace que sea difícil detectar deficiencias en los trabajos existentes y que no sea fácil detectar nuevas necesidades en este campo.

En la primera parte del artículo, se presentará una Revisión Sistemática (RS) de la literatura existente relacionada con el uso de patrones de seguridad para construir arquitecturas tecnológicas seguras, con el fin de detectar las principales deficiencias y necesidades que actualmente existen en este ámbito. Para llevar a cabo esta RS de una manera estructurada y organizada, se han utilizados las guías propuestas por Kitchenham [23, 24] y las plantillas de protocolos de revisión desarrolladas por Biolchini et al. [25] para facilitar la planificación y ejecución de la RS.

Después de llevar a cabo la RS, se realizará un análisis en profundidad del conjunto primario de estudios identificado, el cual ha permitido obtener conclusiones acerca de los métodos de utilización de los patrones de seguridad en arquitecturas seguras y los factores o parámetros que actualmente se tienen en cuenta a la hora de aplicar dichos patrones en los sistemas reales y complejos de una organización. Finalmente, se realizará una discusión de los resultados obtenidos.

El resto del artículo se organizará de la siguiente manera: en la Sección II, se define la cuestión de la investigación. La Sección III describe el método de revisión que está basado en el protocolo de investigación. Se explicará la estrategia de búsqueda y se enunciarán los estudios seleccionados. Además, en esta sección, se definen los datos obtenidos, y se presenta la agrupación realizada en base a los estudios que serán analizados. La Sección IV presenta los resultados y la discusión. Finalmente se expondrán algunas conclusiones en la Sección V.

II. FORMALIZACIÓN DE LA CUESTIÓN

En esta sección, se definirá claramente el objetivo de esta investigación.

A. Foco de la cuestión

El foco de la cuestión está en identificar las iniciativas, estudios e informes basados en experiencias, más relevantes en la disciplina de seguridad en computadores que usan patrones de seguridad para construir arquitecturas tecnológicas seguras en sistemas de información.

B. Calidad de la Cuestión y Amplitud

El gran problema es que en la actualidad existen numerosos patrones de seguridad, como por ejemplo [9, 22], pero no existe una catalogación clara de cuales de los existentes son útiles para analizar o desarrollar arquitecturas de seguridad en los sistemas reales y complejos de una organización. Otro de los problemas importantes es que existen varias alternativas para solventar el mismo problema utilizando patrones de seguridad, es decir, no existe homogeneidad en las propuestas [2, 12], por lo que varios ingenieros de seguridad de la misma organización pueden proporcionar diferentes soluciones al mismo problema, incluso el mismo ingeniero puede seleccionar diferentes alternativas dependiendo del momento, causando que no exista un estrategia de protección alineada dentro de la empresa.

La cuestión de la investigación que dirigirá la búsqueda es la siguiente: ¿Qué estudios se han llevado a cabo para construir arquitecturas tecnológicas seguras utilizando patrones de seguridad? Las palabras clave y los sinónimos que componen esta cuestión y que serán usados durante la ejecución de la revisión son:

- Patrones de seguridad y patrones arquitecturales.
- Arquitecturas tecnológicas y arquitecturas de seguridad.
- Sistemas reales y complejos: Organizaciones, empresas, corporaciones, etc.

Lo que se podrá observar en la RS es cómo los patrones de seguridad son usados en las arquitecturas tecnológicas de organizaciones reales y complejas. Los grupos de población que se han incluido son publicaciones en las fuentes de datos seleccionadas que cubren este ámbito. La selección de fuentes de datos se presentará en la siguiente sección.

El resultado esperado al final de la RS es la identificación de iniciativas relacionadas con los patrones de seguridad usados en arquitecturas tecnológicas de seguridad. Una vez estos estudios han sido identificados, se analizarán siguiendo un *framework* analítico para evaluar su aplicabilidad en sistemas reales y complejos. Los resultados se mostrarán en una tabla para posteriormente establecer una discusión organizada en relación a ellos. La medición de resultados será el número de estudios seleccionados. Las principales áreas de aplicación que se beneficiarán de esta RS serán los ingenieros de seguridad de la información, áreas de seguridad de la información, expertos en el campo de la seguridad de la información, académicos, investigadores y profesionales. Finalmente se obtendrá una visión de la actual situación que permitirá detectar deficiencias y encontrar nuevas necesidades para los patrones de seguridad, con el fin de optimizar la aplicabilidad de estos patrones en el análisis y diseño de sistemas de información seguros.

III. MÉTODO DE REVISIÓN.

Esta sección describe el método de revisión usado. Para llevarlo a cabo, se mostrará cómo se han seleccionado las fuentes y los estudios, y cómo se ha ejecutado la selección para llevar a cabo la RS.

A. Selección de fuentes

Se ha llevado a cabo una primera búsqueda para realizar una estimación del volumen de estudios existentes relacionados con patrones de seguridad usados para construir arquitecturas de seguridad. Por otro lado, también se ha verificado que no existe actualmente una revisión sistemática en este campo.

Los criterios de selección usados para evaluar el estudio de las fuentes son los siguientes: fuentes disponibles que permiten consultar artículos a través de Internet y a través de la librería digital de la Universidad Rey Juan Carlos, que tiene permisos de acceso a "*ACM digital library*", "*IEEE digital library*", "*Science@Direct*", "*SpringerLink*", todas ellas pertenecientes al ámbito de *Computer Sciences*. Todas las librerías digitales deben poseer mecanismos de búsqueda avanzados en los que utilizar palabras claves. Además los estudios deben estar en inglés. Finalmente, las principales fuentes de la lista de fuentes inicial, en las cuales la revisión sistemática ha sido ejecutada son las siguientes: "*ACM digital library*", "*IEEE digital library*", "*Science@Direct*", "*Google Scholar*", capítulos de libros y conferencias relacionadas con este ámbito de seguridad de la información.

B. Selección de Estudios

Una vez definidas las fuentes de búsquedas, es necesario describir la cadena de búsqueda utilizada y los criterios de inclusión y exclusión evaluados para este estudio.

Se han combinado las palabras claves seleccionadas con conectores AND y OR para obtener nuestra cadena de búsqueda. La Fig. 1 muestra la cadena general de búsqueda. Posteriormente se ha alterado dicha cadena de búsqueda con el fin de adaptarla a la sintaxis específica de cada motor de búsqueda.

Security AND (Pattern OR Architecture OR Architectural) AND (Applicability OR Organization OR Corporation OR Enterprise OR Technological OR SMEs OR Real Systems)

Figura 1. Cadena de Búsqueda.

Los criterios de inclusión y exclusión han sido aplicados en el primer conjunto de estudios obtenidos. Por un lado, los criterios de inclusión son los siguientes: se han analizado títulos, palabras clave, *abstracts* y conclusiones de los estudios que describen como se usan los patrones de seguridad en el ámbito concreto de las arquitecturas de seguridad. Por otro lado, los criterios de exclusión para los estudios seleccionados son los descritos a continuación: se ha descartado cualquier estudio que use o describa arquitecturas de seguridad sin utilizar patrones, y se han descartado también cualquier estudio que utilice patrones de seguridad fuera del ámbito de las arquitecturas de seguridad.

Los trabajos incluidos en la revisión final fueron descubiertos a través de un análisis en profundidad de los candidatos, centrándose en el *abstract*, introducción, conclusiones y otras secciones, como las palabras clave y los trabajos relacionados, para identificar las propuestas más relevantes para el estudio. En la mayoría de los casos, se ha leído el artículo completo. Para esta propuesta, se han elegido estudios que están relacionados con la construcción de arquitecturas de seguridad utilizando patrones de seguridad.

C. Ejecución de la Selección

Las búsquedas fueron ejecutadas y la lista inicial de estudios obtenidos fue evaluada acorde con los criterios establecidos. La gestión de la bibliografía de estos estudios obtenidos fue realizada con el paquete bibliográfico EndNote [26]. Después de ejecutar la búsqueda en los diferentes motores de búsqueda, se obtuvieron 360 estudios en total. tarde, estos resultados se filtraron utilizando los criterios de inclusión para proporcionar un conjunto de 71 estudios relevantes. Finalmente después de aplicar los criterios de exclusión, el conjunto final de estudios relevantes consistió en 14 propuestas primarias. Los estudios seleccionados, los cuales cumplen todos los criterios de inclusión y exclusión previamente definidos, son mostrados en Tabla I.

Como se puede ver en la Tabla I, el 42% de los estudios seleccionados corresponden a "*IEEE digital library*", el 28% corresponde a "*ACM digital library*", el 14% a "*Google Scholar*", y otro 14% a "*Science@Direct*".

TABLA I. RESULTADOS OBTENIDOS

	Estudios					
Fuentes	Fecha de busqueda	Descubiertos	No Repetidos	Relevantes	Primarios	%
IEEE Digital Library	05/11/2010	98	77	26	6	42,86%
Google Scholar	09/11/2010	120	56	18	2	14,29%
ACM Digital Library	12/11/2010	79	77	15	4	28,57%
Science@Direct	16/11/2010	63	53	12	2	14,29%
	Total	360	263	71	14	100,00%

D. Extracción de la Información

La información extraída de los artículos analizados contiene diferentes formas de utilizar patrones de seguridad. Debido a las limitaciones de espacio, a continuación exclusivamente se enunciarán las agrupaciones de las propuestas analizadas, las cuales se dividirán en: estudios que exponen metodologías generales para construir arquitecturas seguras usando patrones de seguridad, y estudios en los que se aplican patrones de seguridad en contextos concretos.

En el conjunto de propuestas de metodologías para construir arquitecturas tecnológicas seguras usando patrones de seguridad se encuentran las propuestas [27], [28] y [29].

Por otro lado, en el conjunto de propuestas que usan patrones de seguridad en contextos concretos, se han incluido los siguientes trabajos: [30], [31], [1], [32], [33], [34], [35], [36], [37], [38], y la propuesta [39].

IV. ANÁLISIS DE LOS RESULTADOS.

En esta sección se va a exponer el análisis realizado discutiendo los resultados obtenidos sobre los artículos extraídos de la revisión sistemática. Tanto el análisis como la discusión están enfocados en el modo de utilizar patrones de seguridad para crear arquitecturas tecnológicas seguras en organizaciones reales y complejas. Para este propósito, se analizarán las deficiencias encontradas y las actuales necesidades en este ámbito. El fin es verificar si los patrones de seguridad actuales, propuestos para el análisis o implementación de arquitecturas de seguridad, son útiles para los ingenieros de seguridad encargados de esta tarea en los sistemas de organizaciones reales y complejas. Finalmente, se expondrá un conjunto de sugerencias de mejora en relación a las deficiencias encontradas para que este tipo de soluciones sean óptimamente utilizadas en entornos reales y complejos.

Para llevar a cabo esta tarea, se presenta la Tabla II en la que se comparan las iniciativas seleccionadas.

Para este estudio comparativo, se ha usado un *framewok* analítico (parcialmente basado en [40]). Este *framework* contiene una serie de criterios técnicos de aplicabilidad basados en las consideraciones expuestas por Kienzle et al. [41] , que se detallarán a continuación. Cada uno de los criterios analizados son consideraciones que un ingeniero de seguridad debería tener en cuenta cuando analiza e implementa soluciones de seguridad en los sistemas de una organización real y compleja, ya que dichas consideraciones están relacionadas con parámetros tan importantes como rendimiento del sistema, coste y tiempo empleado en abordar una solución, efectividad y aprendizaje. Para detallar algunas de las consecuencias de no atender estas consideraciones y facilitar además el entendimiento del lector, se presentará un ejemplo breve, claro y real que justificará la necesidad de atender cada una de las consideraciones expuestas.

- ***Impacto en otros componentes*** del sistema: en este criterio se analizará si las propuestas tienen en cuenta las compatibilidades y posibles consecuencias en el resto de componentes del sistema al utilizar un patrón. Para entender este criterio se expone el siguiente ejemplo:
  Como estrategia de seguridad dentro de una organización, se decide llevar a cabo una gestión de identidades centralizada para que desde un único punto, los responsables de seguridad de la organización tengan el control de, por ejemplo, los certificados digitales necesarios para que los sistemas puedan realizar autenticación y puedan establecer relaciones de confianza con los sistemas de otras organizaciones. Una de las posibles soluciones es utilizar un almacén criptográfico único y centralizado independiente del producto o sistema que lo requiera, que albergue dichos certificados de una forma segura. En este caso, si no se tuviese en cuenta compatibilidades entre los elementos existentes en el sistema y la solución a implementar por el patrón de seguridad, podrían surgir problemas como la inviabilidad de la solución. Por ejemplo, si se utilizan algunos productos de Microsoft, como es el caso de Outlook [42], que utiliza certificados para firmar correos electrónicos, debido a que este producto no soporta la integración con ningún almacén criptográfico externo al suyo local, habría que hacer un desarrollo ad-hoc para que el patrón se pudiese implementar en la arquitectura de la organización, y evitar así que los certificados digitales se localicen en diferentes almacenes del sistema.
- ***Impacto en el sistema****:* en este criterio se analizará si las propuestas tienen en cuenta los posibles incrementos surgidos en el sistema involucrado en relación a necesidad de almacenamiento, aumento de memoria consumida, frecuencia de parcheado, capacidad de proceso, ancho de banda, etc. El siguiente ejemplo tratará de exponer el significado de este criterio:
  En una organización se desea implantar un modulo de control de acceso en la arquitectura del sistema de información. Como alternativa se decide utilizar RBAC [9] que se basa en autenticar y autorizar accesos dependiendo del rol que cada usuario/subsistema tenga en una organización. En este caso se debería tener en cuenta los parámetros expuestos anteriormente. Esto es debido a que, dependiendo de la cantidad de usuarios del sistema, la frecuencia de sus accesos y las diferentes combinaciones para posibilitar el acceso a un recurso, las características técnicas de un sistema se pueden ver afectadas. Si no se estima bien, por ejemplo, el volumen de estos usuarios, probablemente se verán afectados el rendimiento del sistema, la capacidad de proceso, el ancho de banda y la memoria consumida, pudiendo causar un colapso en el sistema, y por ende, el fallo de la solución.
- ***Coste de la solución:*** se analizará si se evalúa el coste de instalar o implementar la solución que propone el patrón. Se expondrá un ejemplo conjunto con el siguiente criterio.
- ***Tiempo empleado:*** se chequeará si las propuestas estiman el tiempo necesario, sin necesidad de detalle, para implantar o utilizar un patrón.
  Estos dos criterios se pueden analizar desde una perspectiva conjunta, y además son dependientes de los demás criterios. Esto es debido a que si no se tiene en cuenta algunos de los criterios expuestos en esta sección, estos dos criterios se verán afectados, repercutiendo en la solución. Siempre que no se tienen en cuenta criterios que pueden afectar a la solución final, estos parámetros se pueden ver afectados ya que, por ejemplo, puede aparecer un aumento de costes a posteriori para dimensionar el sistema, y por consiguiente el aumento de tiempo para solucionar un problema con la solución propuesta por el patrón.
- *Exposición* ***ejemplos reales:*** se chequeará si las propuestas están acompañadas de un ejemplo real de implementación que sirva de respaldo para validar la solución. Es evidente que si el patrón dispone en su descripción de un ejemplo real, quiere decir que, por un lado, ha sido implementado en un sistema real, y por otro lado, ha sido testeado verificando su comportamiento como solución.
- Evaluación de la ***criticidad de los activos a proteger***: se analizará si las propuestas catalogan la criticidad del activo a proteger. No todos los activos tienen la misma importancia dentro de una organización, por lo que tratar a todos igual puede repercutir de manera significativa en la solución. Pongamos como ejemplo el caso protección de una aplicación web. Para ello se sugiere la utilización de una secuencia de patrones de seguridad para asegurar la autenticación, autorización, control de acceso basado en roles, además de un cifrado de los datos en las bases de datos para asegurar confidencialidad de éstos. Si la información accesible es de carácter público y la disponibilidad del servicio no es crítica, sobrarían la mayoría de controles ya que, con poner un control perimetral como el patrón *Firewall* [9] bastaría para evitar problemas de ataques de denegación de servicio [4]. Sin embargo si la información accedida es de carácter especial, y su difusión comprometiese a la organización, quizás sería necesario aumentar los controles. Es decir, se debería introducir patrones de seguridad como *Securepipe* [9] y medidas de seguridad adicionales como cifrar los datos en tránsito. Por este motivo, generalizar las soluciones para problemas aparentemente iguales, sin tener en cuenta la

criticidad de los activos a proteger, puede causar ineficiencia o fallo en la solución.

- Cumplimiento de ***Normas y Regulaciones**:* se chequeará si las propuestas tienen en cuenta que las diferente legislaciones de los países donde se implante la solución pueden condicionarla, o si tienen en cuenta cambios en las normas de la organización. A continuación se expone el siguiente ejemplo para aclarar el criterio:
  Supongamos que una empresa tiene diferentes filiales en varios países, y se pretende unificar el sistema de acceso para optimizar el control de acceso a los sistemas de toda la organización. Para ello se propone un repositorio central donde se encuentren las credenciales de todos los usuarios de los sistemas de la organización en todo el mundo. Dependiendo de las regulaciones de cada país, este repositorio común tendrá que tener unas características u otras. Más concretamente, si el repositorio se localiza en países como Argentina, Venezuela o USA, las leyes que aplican a esos países obligan a que estos datos tengan que almacenarse de una determinada forma, que no aplica al resto de países. Además también se pueden dar casos de que esos países no consientan la salida de determinada información de sus usuarios locales, si se decide que el control de acceso se localice en otras sedes de la organización, a no ser que se localice en la sede de la matriz.

Una vez expuestos los criterios a analizar, para cada una de las propuestas seleccionadas, se verificará si cumple completamente el criterio técnico de aplicabilidad evaluado (S), si se refiere brevemente a este criterio (P), o si no menciona ni considera el criterio (N).

En la Tabla II, las columnas verticales muestran las referencias a los artículos analizados y las filas muestran los criterios expuestos anteriormente.

TABLA II. ANALISIS DE PROPUESTAS

		Criterios Técnicos de Aplicabilidad						
		Impacto en otros componentes	*Impacto en el sistema*	*Coste de la solución*	*Tiempo empleado*	*Ejemplos reales*	*Criticidad de los activos*	*Normas y Regulaciones*
Propuestas	[28]	N	P	N	N	P	N	N
	[36]	N	N	N	N	S	N	N
	[27]	N	N	N	N	P	N	N
	[30]	P	S	N	N	S	N	S
	[1]	N	P	N	N	N	S	N
	[32]	N	P	N	N	N	S	S
	[39]	N	N	N	N	N	N	N
	[38]	N	N	N	N	P	N	N
	[37]	N	N	N	N	P	N	N
	[33]	N	P	N	N	S	N	N
	[31]	N	N	N	N	P	N	N
	[34]	N	P	N	N	P	N	N
	[35]	S	S	S	N	N	N	N
	[29]	N	P	N	N	P	N	N

Como se puede extraer de la Tabla II, la mayoría de las propuestas carecen de:

a) Una evaluación de las compatibilidades y posibles consecuencias sobre el resto de los componentes del sistema cuando se usa un patrón de seguridad en él. Se puede observar que sólo una propuesta menciona que podrían verse afectados componentes del sistema [30], sin especificar cuáles ni en qué medida, y otra de las propuestas expone claramente el impacto que tendría el patrón en los diferentes elementos de un sistema [35]. Esta deficiencia puede causar incompatibilidades con algunos de los elementos de la arquitectura del sistema al no ser detectados a priori provocando en algunos casos el fallo de la solución; b) Una evaluación detallada del impacto que el patrón podría tener en el sistema dónde es introducido, en términos de almacenamiento, consumo de memoria, frecuencia de parcheado, capacidad de proceso, ancho de banda, etc. En este caso, existen propuestas que mencionan una posible alteración en el sistema dónde se implementa la solución en forma de patrón, pero sin dar detalles de esta situación [28], [1], [32], [33], [34], y [29]. En cambio, dos propuestas exponen claramente las posibles mermas del sistema al introducir el patrón [30], y [35]. Es importante destacar que la ausencia del análisis de estos parámetros críticos podría comprometer la disponibilidad del servicio; c) Una clasificación específica de la criticidad de los activos que deben ser protegidos por el patrón. En este caso, dos propuesta tiene en cuenta este parámetro, exponiendo claramente diferentes medidas en base a la criticidad del activo que debe proteger el patrón utilizado [1] y [32]. Si este parámetro no es analizado, el riesgo de no seleccionar apropiadamente las medidas de seguridad a adoptar aumentan, causando excesivas inversiones en seguridad, o en su defecto, dejando el sistema vulnerable ante cualquier ataque no tenido en cuenta en las primeras etapas del diseño; d) Una presentación general del impacto en coste y tiempo necesario para implantar el patrón. En relación a este parámetro, sólo una propuesta tiene en cuenta que la implementación del patrón de seguridad dentro de un sistema podría aumentar los costes asociados al utilizar dicha solución [35]. Esta deficiencia en los análisis de problemas reales podría causar que una organización descartase la solución porque no se pudiese asumir el coste asociado a ella, o porque al no disponer de plazos precisos, sea imposible realizar una estrategia de negocio a corto plazo; y finalmente, e) consideraciones específicas relacionadas con las limitaciones que pueden ser impuestas por las normas y regulaciones de los diferentes países donde se encuentran los sistemas de la organización. En este caso, dos propuestas mencionan este aspecto con claridad [30] y [32], exponiendo que habría que tener en cuenta la localización y el sector donde opera la organización a la hora de implementar la solución propuesta. Cuando el negocio de una organización depende de, entre otros factores, las regulaciones de los países donde los sistemas son localizados, es necesario incluir esta variable en la ecuación ya que puede condicionar la solución.

Todos estos parámetros son críticos, y por ende, condicionantes a la hora de utilizar patrones de seguridad en

las arquitecturas de los sistemas reales de una organización. La ausencia de su análisis, en la mayoría de los casos, puede provocar el fallo de la solución.

Pese a los resultados del análisis, desde nuestro punto de vista, los patrones de seguridad son una buena herramienta para homogeneizar soluciones de seguridad entre diferentes ingenieros ante problemas similares y, para aportar soluciones ágiles, probadas, validadas y seguras ante problemas de seguridad recurrentes. Pero, por otro lado, tras este análisis consideramos que queda mucho trabajo por realizar para que el uso de patrones de seguridad sea una práctica común a la hora de realizar los diseños de arquitecturas de seguridad en sistemas de información de organizaciones reales y complejas.

Por este motivo, y por todos los argumentos expuestos en los párrafos anteriores, nosotros creemos necesario que los patrones de seguridad actuales evolucionen hasta reflejar cada una de las consideraciones expuestas. Por otro lado, también creemos necesario la creación de patrones de seguridad específicos para su uso en arquitecturas de seguridad, en los cuales se reflejen también todas y cada una de las consideraciones expuestas, para conseguir que su utilización cumpla con las necesidades actuales de las organizaciones.

Finalmente, nosotros queremos destacar la importancia de disponer de procesos sistemáticos que guíen paso a paso a los ingenieros de seguridad a construir sistemas reales seguros con la ayuda de patrones de seguridad. De esta manera se garantizará la seguridad de los sistemas de información de una organización, y se conseguirá que todas las soluciones adoptadas en materia de seguridad sigan una estrategia alineada dentro de las distintas sedes de una organización.

V. CONCLUSIONES.

El principal objetivo de este artículo fue realizar una revisión sistemática de la literatura existente relacionada con el uso de patrones de seguridad en el análisis y diseño de arquitecturas de seguridad en sistemas reales y complejos de grandes organizaciones. Posteriormente se realizó un análisis de los resultados en el que se detectaron las principales deficiencias y necesidades de investigación en este ámbito.

La revisión sistemática fue realizada siguiendo una serie de guías, propuestas por diferentes autores, que han sido aceptadas y validadas por la comunidad científica. Esto aseguró que la revisión fue realizada de una forma estructurada y organizada, y facilitó su planificación y ejecución.

La principal conclusión de esta investigación es que las propuestas actuales que utilizan patrones de seguridad dentro de las arquitecturas tecnológicas de organizaciones reales y complejas, no tienen en cuenta consideraciones que pueden condicionar la solución, y por lo tanto críticas. Es decir, no tienen en cuenta el impacto que el patrón puede tener en el sistema o en alguno de sus componentes; no realizan una clasificación de la criticidad de los activos a proteger generalizando las soluciones de forma ineficiente; y, no tienen en cuenta las diferentes regulaciones y normas existentes en diferentes países. La ausencia del análisis de estas y otras consideraciones expuestas en el artículo pueden causar un incremento drástico en términos de coste y tiempo al abordar un problema de seguridad, y en algunos casos el fallo de la solución. Por eso creemos que queda mucho trabajo por hacer para lograr que este tipo de soluciones sean adoptadas en organizaciones reales.

Nuestra propuesta actual está centrada en el desarrollo y depuración de una nueva plantilla para la creación de patrones de seguridad para arquitecturas tecnológicas que se puede encontrar en [43]. En esta plantilla se reflejan todos los parámetros expuestos en el análisis anterior. Por eso, su utilización para definir nuevos patrones de seguridad aportará al ámbito de arquitecturas de seguridad en organizaciones reales un catálogo de soluciones a problemas recurrentes. Estas soluciones no sólo ofrecerán mecanismos para agilizar la toma de decisiones cuando surja un nuevo problema, sino que además evitará problemas asociados al impacto del uso de los patrones de seguridad en sistemas reales.

Por otro lado, nosotros estamos trabajando en la definición de un proceso sistemático soportado por patrones de seguridad, adicional a las metodologías de *software* tradicionales, con el fin de asistir paso a paso a los ingenieros a la hora de construir sistemas de información seguros o mantener el nivel de seguridad alcanzado en los sistemas de información de una organización de forma organizada, iterativa e incremental.

REFERENCIAS

[1] E.B. Fernandez, et al., "On building secure SCADA systems using security patterns". En CSIIRW '09: Proceeding of the Annual Workshop on Cyber Security and Information Intelligence Research. ACM, NY, USA (2009), pp. 1-4.

[2] S. Moral-Garcia, et al., "Patrones de Seguridad: ¿Homogéneos, validados y útiles?". RECSI '10, Spain, 2010.

[3] E.B. Fernandez and R. Pan, "A pattern language for security models " *PLoP*, 2001, pp. 13.

[4] "The Open Web Application Security Project (OWASP)," 2011; http://www.owasp.org.

[5] "SANS - Computer Security Training, Network Research & Resources," 2011; http://www.sans.org/.

[6] "Internet Crime Complaint Center. IC3," 2010; www.ic3.gov.

[7] G. Stoneburner, et al., "Risk Management Guide for Information Technology Systems," *NIST Special Publication 800-30*, 2002.

[8] E. Gamma, et al., "*Design Patterns: Elements of Reusable Object Oriented Software*," *Addison Wesley*, 1995.

[9] M. Schumacher, et al., *Security Patterns: Integrating Security and Systems Engineering*, 2006.

[10] C. Alexander, et al., "*A Pattern Language: Towns, Buildings, Constructions*," *Oxford University Press*, 1977.

[11] M. Fowler, "*Analysis Patterns: Reusable Object Models*," *Adisson Wesley*, 1997.

[12] R. Ortiz, et al., "Applicability of Security Patterns". On the Move to Information Systems 2010: OTM 2010 Workshops, 2010.

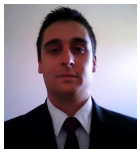
[13] J. Yoder and J. Barcalow, "Architectural Patterns for Enabling Application Security," *Fourth Conference on Patterns Languages of Programs (PLoP'97)*, 1997.

[14] Z. Anwar, et al., "Multiple design patterns for voice over IP (VoIP) security," *Proc. Performance, Computing, and Communications Conference, 2006. IPCCC 2006. 25th IEEE International*, 2006.

[15] E.B. Fernandez, et al., "Even more patterns for secure operating systems". Proceedings of the 2006 conference on Patterns languages of programs. ACM, Portland, Oregon, 2006.

[16] S. Halkidis, et al., "Quantitative Evaluation of Systems with Security Patterns Using a Fuzzy Approach," *On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops*, 2006, pp. 554-564.

[17] J. Dong, et al., "Automated verification of security pattern compositions," *Information and Software Technology*, vol. In Press, Corrected Proof.
[18] A. Sarmah, et al., "Security Pattern Lattice: A Formal Model to Organize Security Patterns," *Proc. DEXA '08. 19th International Conference on Database and Expert Systems Application*, 2008, pp. 292-296.
[19] E.B. Fernandez, et al., "Classifying security patterns," *Proc. 10th Asia-Pacific web conference on Progress in WWW research and development*, 2008, pp. 342-347.
[20] P. El Khoury, et al., "An Ontological Interface for Software Developers to Select Security Patterns," *Proc. DEXA '08. 19th International Conference on Database and Expert Systems Application*, 2008, pp. 297-301.
[21] M. Weiss and H. Mouratidis, "Selecting Security Patterns that Fulfill Security Requirements," *Proc. RE '08. 16th IEEE International Requirements Engineering* 2008, pp. 169-172.
[22] D.M. Kienzle, et al., "Security patterns repository, version 1.0," 2006.
[23] B. Kitchenham, "*Guideline for performing Systematic Literature Reviews in Software Engineering. Version 2.3*," *University of Keele (Software (Software Engineering Group, School of Computer Science and Mathematics) Mathematics) and Durham (Dep. of Computer Science)*, 2007.
[24] B. Kitchenham, "*Procedures for Perfoming Systematic Review*," *Joint Technical Report, Software Engineering Group, Dep. of Computer Scinece Keele University, U.K. and Empirical Software Engineering, National ICT Australia Ltd.: Australia.*, 2004.
[25] J. Biolchini, et al., "*Systematic Review in Software Engineering*," *Systems Engineering and Computer Science Department COPPE / UFRJ: Rio de Janeiro*, 2005.
[26] "EndNote Web," 2010; http://www.endnote.com/.
[27] Jan Jurjens, "Foundations for Designing Secure Architectures," *Electron. Notes Theor. Comput. Sci.*, vol. 142, 2006, pp. 31-46; DOI 10.1016/j.entcs.2005.07.012.
[28] Eduardo B. Fernandez et al., "Using security patterns to build secure systems", pp., 2.
[29] Eduardo B. Fernandez et al., "Using security patterns to develop secure systems," H. Mouratidis (ed.): Software Engineering for Secure Systems: Industrial and Research Perspectives, pp. 16-31, 2009 .
[30] P. Busnel, et al., "S&D Pattern Deployment at Organizational Level: A Prototype for Remote Healthcare System," *Electronic Notes in Theoretical Computer Science*, vol. 244, 2009, pp. 27-39.
[31] S.G. Brown and F. Yip, "Integrating Pattern Concepts & Network Security Architecture," *Proc. NOMS '06:10th IEEE/IFIP Network Operations and Management Symposium*, 2006, pp. 1-4.
[32] E.B. Fernandez, M.M. Larrondo-Patrie, "Designing Secure SCADA Systems Using Security Patterns " *Proc. 43rd Hawaii International Conference on System Sciences (HICSS).* 2010, pp. 8.
[33] D. Bellebia and J.M. Douin, "Applying patterns to build a lightweight middleware for embedded systems". Proceeding of the 2006 conference on Pattern languages of programs. ACM, Portland, Oregon (2006).
[34] E.B. Fernandez, et al., "Security Patterns for Voice over IP Networks," *Proc. ICCGI '07. International Multi-Conference on Computing in the Global Information Technology*, 2007, pp. 33-33.
[35] Q. Xiangli, et al., "Integration Patterns of Grid Security Service". Proceedings of the Sixth International Conference on Parallel and Distributed Computing Applications and Technologies, IEEE Computer Society (2005).
[36] D. Lirong and C. Kendra, "Using FDAF to bridge the gap between enterprise and software architectures for security," *Sci. Comput. Program.*, vol. 66, no. 1, 2007, pp. 87-102; DOI 10.1016/j.scico.2006.10.010.
[37] M. Schnjakin, et al., "A pattern-driven security advisor for service-oriented architectures". Proceeding of the 2009 ACM workshop on Secure Web Services. AMC, Chicago, Illinois, USA (2009).
[38] M. Michael, et al., "A Pattern-Driven Generation of Security Policies for Service-Oriented Architectures". Proceedings of the 2010 IEEE International Conference on Web Services, IEEE Computer Society (2010).
[39] N. Delessy, et al., "A Pattern Language for Identity Management," *Proc. ICCGI '07. International Multi-Conference onComputing in the Global Information Technology.*, 2007, pp. 31-31.
[40] A. Khawaja and J. Urban, "A synthesis of evaluation criteria for software specifications and specifications techniques," *International Journal of Software Engineering and Knowledge Engineering*, vol. 12, no. 5, pp. 581-599.
[41] D.M. Kienzle, et al., "Security patterns template and tutorial," 2002.
[42] Microsoft Outlook, 2011.
[43] S. Moral-García, et al., "A New Pattern Template to Support the Design of Security Architectures," The Second International Conference of Pervasive Patterns and Applications, PATTERNS '10, Lisbon, Portugal (2010).



Roberto Ortiz received the Engineering degree in Computer Science, Master degree in Information Systems and IT, and Master degree in Decision Engineering by the Universidad Rey Juan Carlos, Madrid, in 2007, 2008, and 2009, respectively. Currently he is a PhD student in Computer Science in the field of information security, in the same institute. His current research interest are security in information systems, especially in security patterns used in real environments, and security methodologies to optimize the process of development of secure systems in real and complex organization. In 2007, Mr. Ortiz started to work at BBVA Group, firstly, in the e-fraud Prevention Team, and at present he serves as security analyst and security architect.

Santiago Moral-Rubio is IT Engineer by the Universidad Politécnica de Madrid, in Spain. In 2008, he achieves the Master in Information Systems and IT by the Universidad Rey Juan Carlos in Madrid, Spain). The next year, he obtains the degree on Master in Decision Engineering, in the same Universidad Rey Juan Carlos. Mr. Moral is currently preparing the Doctorate in Risk Management of Intentionality. He is focusing on the application of Game Theory to the intentionality of Organised Crime, as the main analysis axis of risks with an adversary. He is ISACA certified as CISA, CISM and CGEIT. Since 2001, Mr. Moral serves as BBVA Group CISO. He is responsible for overall planning, design and implementation of IT Security, Logical Security, Information Security, e-fraud Prevention, IT Governance, Risk and Control in all BBVA Group interests.

Javier Garzás received his M.S. (2000) and Ph.D. (2004) degrees in computer science from the University of Castilla-Castilla-La Mancha (UCLM). He is currently the CEO of Kybele-Consulting and associate professor at Rey Juan Carlos University. His research interests include capability maturity model, object-oriented design, and software process and project management.

Eduardo Fernández-Medina holds a PhD. and an MSc. in in Computer Science from the University of Sevilla. He is Associate Professor at the Escuela Superior de Informática of the University of Castilla-La Mancha at Ciudad Real (Spain), his research activity being in the field of security in 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 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. He belongs to various professional and research associations (ATI, AEC, AENOR, IFIP WG11.3, etc.).