BIG DATA E INTELIGENCIA ARTIFICIAL APLICADA A LA SEGURIDAD

Definiendo Métricas para la Gestión Dinámica del riesgo, mediante la metodología MARISMA

Luis E. Sánchez, Antonio Santos-Olmo, Julio Moreno, Manuel Serrano, David G. Rosado, Eduardo Fernández-Medina

Resumen – En una sociedad en que los sistemas de Análisis y Gestión del riesgo son cada vez más necesarios para la correcta Gestión de la Seguridad de las compañías, surge la problemática de cómo hacer que estos sistemas pueden evolucionar y aprender de una forma natural, contando con la mayor información posible. Esta evolución del riesgo tiene que estar asociada con los eventos que ocurren dentro de la compañía, tanto los que pueden ser automatizados como los que deben gestionarse de forma manual, pero también debe poder asociarse con los riesgos externos que cambian con el tiempo. En este artículo presentamos algunas de las métricas que se han definido dentro de la metodología MARISMA (Methodology for the Analysis of Risks on Information System, using Meta-Pattern and Adaptability), con el objetivo de conseguir que los análisis de riesgos sean capaces de evolucionar de forma dinámica teniendo en cuenta elementos internos y externos, incluso los asociados con riesgos de terceras compañías.

Palabras clave — Cibersecurity, Information Systems Security Management, ISRA, Information Security Risk Analysis, ISMS, Risk Analysis.

I. INTRODUCCIÓN

Hoy en día, los elementos digitales o las infraestructuras (computadoras, redes, contenidos, etc.) son elementos cada vez más complejos y dependientes de las TI, que están en el centro de nuestras vidas y constituyen los pilares esenciales de nuestras infraestructuras de comunicación, económicas, sociales e institucionales [1]. La seguridad y la mitigación de amenazas dentro de esos sistemas se ha convertido implícitamente en una parte fundamental para el ciudadano (para preservar su privacidad), para la empresa (para proteger los activos y transacciones digitales) y para los estados (para proteger sus infraestructuras críticas y asegurar la continuidad del gobierno y servicios gubernamentales, etc.) [2, 3].

Esta seguridad es cada vez más importante en entornos como el sector salud, las PYMES, las Infraestructuras Críticas, las Industrias asociadas con la Industria 4.0, o en los propios ciudadanos con la aparición de conceptos como el IoT y los sistemas ciberfísicos [4, 5].

Para proteger estos sistemas recurrimos a la gestión de la seguridad, que según [6] puede definirse como un sistema de gestión usado para establecer y mantener un entorno seguro de la información. El objetivo principal de un SGSI (Sistema de Gestión de Seguridad de la Información) es afrontar la puesta en práctica y el mantenimiento de los procesos y procedimientos necesarios para manejar la seguridad de las tecnologías de la información. Estas acciones incluyen la identificación de las necesidades de seguridad de la información y la puesta en práctica de estrategias para satisfacer estas necesidades, medir los resultados y mejorar las estrategias de protección.

La definición de un SGSI es una tarea ardua y compleja que requiere un proceso previo de definición en la compañía donde se quiere establecer. Una de las fases más importantes para la implantación de un SGSI es la de Análisis y gestión de riesgos, que para algunos investigadores es una de las fases más críticas [7].

Todas las organizaciones que utilizan tecnologías de la información tienen problemas con la seguridad de su sistema de información. El primer paso en el proceso de protección de un sistema de información es la identificación y clasificación de los recursos o activos de información que necesitan protección, porque son vulnerables a las amenazas, y para realizar este paso necesitamos contar con sistemas de análisis y gestión de riesgos adecuados [8]. Diferentes investigadores destacan que la gestión de riesgos es un proceso esencial en cualquier modelo de gestión empresarial [9, 10], y que la información es un activo valioso que se espera que esté protegido.

Un análisis de riesgos es un proceso sistemático para estimar la magnitud de los riesgos a los que está expuesta una organización, para saber qué decisión tomar ante una posible eventualidad [11]. Para ello, se seleccionan e implementan salvaguardas para poder conocer, prevenir, impedir, reducir o controlar los riesgos identificados. Esto es lo que se entiende como gestión de riesgos.

De forma más técnica, el análisis de riesgos permite determinar cómo es, cuánto vale y cómo de protegidos se encuentran los activos. En coordinación con los objetivos, estrategia y política de la organización, las actividades de gestión de riesgos permiten elaborar un plan de seguridad que, implantado y operado, satisfaga los objetivos propuestos con el nivel de riesgo que acepta la dirección.

Actualmente se están realizando muchas investigaciones sobre análisis de riesgos, y muchas de ellas intentan comparar los métodos clásicos para ver cómo se podrían alinear [12-18]. Otros investigadores han realizado también algunos análisis comparativos de los principales estándares de riesgos con el

L. E. Sánchez, Grupo de Investigación GSyA, Universidad de Castilla-la Mancha, Ciudad Real, España, Luisenrique@sanchezcrespo.org

A. Santos-Olmo, Departamento I+D+i, Sicaman Nuevas Tecnologías y Marisma Shield, Tomelloso (Ciudad Real), España, Asolmo@sicaman-nt.com

Julio Moreno, Grupo de Investigación GSyA, Universidad de Castilla-la Mancha, Ciudad Real, España, Julio.moreno@uclm.es

Manuel A. Serrano, Grupo de Investigación Alarcos, Universidad de Castilla-la Mancha, Ciudad Real, España, Manuel.serrano@uclm.es

D.G. Rosado, Grupo de Investigación GSyA, Universidad de Castilla-la Mancha, Ciudad Real, España, David.Grosado@uclm.es

E. Fernandez-Medina, Grupo de Investigación GSyA, Universidad de Castilla-la Mancha, Ciudad Real, España, Eduardo.FdezMedina@uclm.es

objetivo de mejorar algunos de sus aspectos [19, 20].

Uno de los principales puntos que destacan las metodologías existentes, es la necesidad de poder contar con sistemas de riesgos que sean capaces de evolucionar y aprender de la experiencia. Así, Dehkhoda [21] analiza la posibilidad de unir métodos tradicionales de análisis de riesgos como IRAM2 con los análisis CBA (Cost-Benefit Analysis), ya que entiende que los unos no pueden funcionar sin los otros. Wangen [22] plantea la necesidad de contar con métricas que puedan ser valoradas en entornos profesionales. Según Pandey [23], cualquier activo de información, cuando está conectado al mundo exterior, es vulnerable a los ataques y estos ataques deben ser identificados lo antes posible. López [24] se centra en el Riesgo Dinámico y destaca que la aplicación de procesos de Análisis y Gestión de Riesgos en el ámbito de los Sistemas de Información es una práctica común que permite la planificación en un momento puntual de tiempo de las acciones preventivas frente al riesgo a corto, medio o largo plazo, pero con un considerable potencial actualmente desaprovechado para facilitar la toma de decisiones en tiempo real frente a eventos o incidentes de seguridad. Este trabajo hace un recorrido por las principales corrientes que buscan sacar partido a este potencial, englobadas principalmente bajo el concepto de Análisis de Riesgos Dinámico.

Otros investigadores no sólo destacan la necesidad de contar con sistemas dinámicos, sino también con sistemas que sean capaces de adaptarse a los entornos cambiantes. De esta forma, Saripalli [25] plantea la necesidad de modernizar los modelos de riesgos para que se puedan adaptar a entornos como el Cloud Computing [25], y Li y Sicari [26, 27] proponen la necesidad de avanzar en el análisis de riesgos para IoT, tanto desde el punto de vista de modernizar los modelos existentes como de la necesidad de añadir sistemas inteligentes de valoración del riesgo, tales como las redes neuronales.

Después de analizar estas propuestas, vemos que es necesario poder contar con sistemas y mecanismos que nos permitan generar sistemas de gestión de riesgos que tengan la capacidad de aprender y evolucionar de forma constante, mediante el análisis y la inclusión de todas las variables de su entorno. No sólo las variables internas, sino también las variables externas, y en este aspecto es importante incluir los ataques que sufren otras empresas de su entorno y tipología.

Para cumplir con todos estos aspectos, es necesario afrontar el desarrollo de una estructura de procesos que permita relacionar todos estos elementos y un conjunto de métricas que les dé soporte.

El resto del artículo se estructura de la siguiente forma: En la Sección 2 se analizarán los procesos principales que conforman la metodología MARISMA, y cómo estos elementos se relacionan entre sí para transmitir la información y el conocimiento generado. En la Sección 3, se presentarán el conjunto de métricas e indicadores iniciales que han sido desarrollados para cumplir con los objetivos de la investigación, explicando cada uno de los cinco bloques en que se dividen. Finalmente, en la última sección describiremos las principales conclusiones obtenidas.

II. METODOLOGÍA MARISMA

En este apartado explicaremos las bases sobre las que se sustenta la metodología de MARISMA, y para ello se mostrará una visión general de los procesos que conforman la metodología.

Figura - 1. Visión general de los procesos de la metodología

La metodología MARISMA está constituida por tres Procesos (ver Figura 1), que a su vez se dividen en actividades, tareas y sub-tareas:

- *Proceso 1 – Generación de Patrones para el Análisis de Riesgos (GPRA):* Se establece una estructura de relaciones entre los diferentes elementos involucrados en el análisis de riesgos y los controles necesarios para gestionar la seguridad. Estas relaciones se establecen mediante el conocimiento adquirido en las diferentes implantaciones, que es almacenado en una estructura denominada patrón para ser reutilizado con posterioridad, reduciendo los costes de generación de este proceso.
- *Proceso 2 – Generación del Análisis y Gestión del Riesgo (GARM):* Mediante la selección del patrón más adecuado y la identificación de un pequeño conjunto de los principales activos se obtiene un detallado mapa de la situación actual (análisis del riesgo) y un plan de recomendaciones de cómo mejorarlo (gestión del riesgo).
- *Proceso 3 – Mantenimiento Dinámico del Análisis de Riesgos (DRM):* Mediante la utilización de las matrices generadas, las cuáles interconectan los diferentes artefactos, el sistema irá recalculando el análisis de riesgos según se produzcan incidentes de seguridad, fallen las métricas definidas o los auditores detecten “no conformidades” en los controles.

En la Figura 2 se puede ver los tres procesos que componen la metodología MARISMA, y cómo intercambian información entre ellos para hacer evolucionar el sistema. A continuación explicaremos de forma resumida cada uno de los

elementos que la conforman, tomando como punto de partida la “Generación de un evento” en el tercero de los procesos, que es el elemento que provoca la “reacción evolutiva/adaptativa” en los demás:

- *Paso 1* – La generación de un evento en el proceso DRM provoca que la instancia de Análisis de Riesgos asociada al evento, generada mediante el proceso GARM, evolucione cambiando aspectos como el nivel de cobertura de un control, o la probabilidad de ocurrencia de una amenaza.
- *Paso 2* - La generación de un evento en el proceso DRM provoca cambios en el patrón asociado a la instancia que se creó mediante el proceso GPRA, permitiéndole reajustar las relaciones entre sus elementos.
- *Paso 3* - La generación de un evento en el proceso DRM provoca cambios en el patrón asociado a la instancia que se creó mediante el proceso GPRA, permitiéndole reajustar elementos asociados al riesgo externo temporal, ayudando a crear un escudo de seguridad global entre las compañías que usan ese patrón.
- *Paso 4* – Los cambios en el patrón provocados en el Paso 2 hacen que los patrones asociados por ley de herencia en las que se basa la metodología, también evolucionen, transmitiendo el conocimiento adquirido.
- *Paso 5* – Los cambios/evolución de todos los patrones, se transmiten a todas las instancias para ayudarles a mejorar y evolucionar.

Figura - 2. Flujo de Generación de Conocimiento en MARISMA

Este ciclo permite, mediante la utilización de estos tres procesos, una constante evolución de las instancias

(individuos) y de los propios patrones (especie), haciendo que el sistema siempre evolucione con los cambios.

Estos tres procesos se dividirán en actividades y tareas, generando artefactos y relaciones entre ellas. La construcción de estos tres procesos, busca solucionar de forma total/parcial los problemas identificados durante la investigación.

III. MÉTRICAS PARA EL AR EN MARISMA

En este apartado se expone el conjunto de indicadores, reglas de negocio y métricas que han sido desarrolladas para poder dotar de dinamismo a la metodología MARISMA,

El objetivo último perseguido en esta fase es ser capaces de localizar y desarrollar indicadores y métricas que nos permitan calcular de forma semi-automática los valores asociados al nivel de riesgo, reduciendo el nivel de incertidumbre en la elaboración del análisis de riesgos.

Dentro del conjunto de métricas iniciales asociadas con la metodología MARISMA podemos distinguir cinco bloques:

- *Métricas asociadas al Patrón:* Son el conjunto de métricas que permitirán establecer relaciones de dependencia entre de los diferentes elementos del patrón (Ej: las dependencias entre los controles, las amenazas y los activos).
- *Métricas asociadas al Análisis de Riesgos:* Son el conjunto de métricas que utilizaremos para reajustar los valores asociados al Análisis de Riesgo y para realizar el cálculo del riesgo.
- *Métricas asociadas al Escudo de Seguridad Global (Global Security Shield – GSS):* Son el conjunto de métricas que nos permitirán crear una visión global del riesgo de cada elemento en un instante de tiempo dado, de forma asociativa entre todas las instancias relacionadas.
- *Métricas asociadas con la Sondas:* Son métricas asociadas con sondas (herramientas externas) que permiten el seguimiento automatizado de vulnerabilidades asociadas con controles.
- *Métricas asociadas a la valoración de los Activos:* Son métricas que nos permitirán calcular, de la forma más objetiva posible, el valor que tiene un activo de información para una compañía.

A continuación analizaremos las métricas de cada uno de estos bloques.

A. Métricas asociadas al Patrón.

Los patrones en Marisma, se basan en tres elementos principales (Controles, Activos y Amenazas) y existen relaciones entre ellos, tanto consigo mismos (Amenaza x Amenaza), como entre elementos de diferentes naturaleza (Control x Amenaza). Las métricas asociadas con el patrón tienen por objetivo determinar los grados de vinculación entre los elementos del patrón. Así por ejemplo, las dependencias entre Controles x Controles reflejaran una estadística de las dependencias asociadas a los eventos ocurridos por las instancias relacionadas con ese patrón.

Se definen inicialmente tres métricas para este tipo de relaciones:

- *Asociadas con los Controles:*
 - *Porcentaje de Inter-dependencias entre controles - Percentage of Inter-dependencies Between Controls (PIBC):* Define la relación que existe entre dos controles.
 - $PIBC = [n^{\circ} \text{ eventos en que aparecen ambos controles}] * 100 / [n^{\circ} \text{ eventos}]$
- *Asociadas con los Tipos de Activos:*
 - *Porcentaje de Inter-dependencias entre tipos de activos - Percentage of Inter-dependencies Between Types of Assets (PIBTA):* Define la relación que existe entre dos tipos de activos.
 - $PIBTA = [n^{\circ} \text{ eventos en que aparecen ambos tipos de activos}] * 100 / [n^{\circ} \text{ eventos}]$
- *Asociadas con las Amenazas:*
 - *Porcentaje de Inter-dependencias entre amenazas - Percentage of inter-dependencies between threats (PIBT):* Define la relación que existe entre dos amenazas.
 - $PIBT = [n^{\circ} \text{ eventos que en aparecen ambas amenazas}] * 100 / [n^{\circ} \text{ eventos}]$

Las dependencias entre matrices permitirán conocer mucho mejor la dependencia entre este tipo de elementos y ser la base para el desarrollo de un sistema experto que recomiende elementos complementarios a un usuario al rellenar un evento (Ej: Si el nivel de dependencia entre dos tipos de controles es del 75%, y en un evento añadimos uno de ellos, el sistema podrá indicar al usuario si está seguro de que el otro control no ha estado involucrado también en el evento de seguridad).

El segundo conjunto de métricas asociadas con esta parte estará orientada las relaciones inter-objetos, es decir entre objetos diferentes:

- *Métricas asociadas con las Amenazas y Controles:*
 - *Porcentaje de Inter-dependencias entre una amenaza y un control - Percentage of Inter-Dependencies Between a Threat and a Control (PIDBTC):* Define la relación que existe entre una amenaza y un control. Esta métrica es no modificable y sólo se mostrará sus resultados a nivel informativo.
 - $PIDBTC = [N^{\circ} \text{ de Amenazas en un evento que han activado ese Control}] * 100 / [n^{\circ} \text{ de veces que esa amenaza ha ocurrido en un evento}]$
 - *Porcentaje de Inter-dependencias entre una amenaza y un control por evento - Percentage of Inter-dependencies between a threat and an event control (PIBTEC):*

- $PIBTEC = \text{Al ocurrir una amenaza en un evento, para cada control involucrado:}$

⇒ Si existe la relación => Valor Actual + 1% (hasta un max de 100%).

⇒ Si no existe la relación => Valor Actual = 1%.

⇒ Para aquellos controles que están relacionados con la amenaza en la matriz pero no en el evento. Valor Actual – 1%.

- *Métricas asociadas con los Tipos de Activos, Amenazas y Dimensiones:*

- *Valor del Porcentaje de Degradación de la Dimensión de un Activo - Value of the Degradation Percentage of the Dimension of an Asset (VDPDA).*

- $VDPDA = \text{Valor medio del rango del evento.}$

B. Métricas asociadas al Análisis de Riesgos.

Una instancia de un análisis de riesgos debe tener dos objetivos principales:

- Capacidad de calcular el riesgo.
- Capacidad de adaptación del riesgo y sus elementos ante cambios.

Para calcular el riesgo, existen diferentes fórmulas que se pueden utilizar, aunque inicialmente la metodología MARISMA ha configurado la siguiente:

- $\text{Nivel Riesgo Actual} = ([\text{Valor Activo}] \times [\text{Max (Impacto Dimensiones)}]) * [\text{Probabilidad de ocurrencia}] * [\text{Vulnerabilidad}]$, calculándose la vulnerabilidad a partir de la ausencia del nivel de cobertura de los controles. El nivel de riesgo se mueve en un rango de [1-500].

El Nivel de Riesgo Actual se transformará a una Escala de Riesgo de 10 niveles, en base a una escala logarítmica, que se calcula aplicando la fórmula indicada en la Ecuación 1.

$$\begin{aligned}
 y &= a^x \\
 500 &= a^{10} \\
 \log 500 &= 10 \log a \\
 \log a &= \frac{\log 500}{10} = 0,26989700 \\
 a &= 10^{0,26989} = 1,8616455 \\
 y &= a^x \rightarrow x = \frac{\log y}{\log 1,86164}
 \end{aligned}$$

Ecuación 1. Cálculo de niveles para riesgo.

Los resultados de aplicar la Ecuación 1 sobre una escala de riesgo máximo de 500 se puede ver de forma numérica y gráfica en la Figura 3.

Figura - 3. Escala logarítmica para el cálculo de niveles de riesgo.

Este es sólo un ejemplo de métrica que nos puede permitir calcular el riesgo. Existen otras métricas que podríamos llegar a aplicar, por lo que se ha buscado que la metodología MARISMA extraiga los valores de los niveles de controles, vulnerabilidades, valoración de activos y amenazas, con el objetivo de poder hacer extensivas sus métricas, de forma que dé cabida a las métricas recomendadas por otros estándares, como:

- CRAMM (Central computer and Telecommunication Agency Risk Analysis and Management Method) [28, 29]:
 - $CRAMM = [Riesgo (Amenaza, Activo) = Probabilidad (Amenaza) * Vulnerabilidad (Amenaza, Activo) * Impacto (Amenaza, Activo)]$
- MEHARI (Méthode Harmonisée d'Analyse de Risques—Harmonised Risk Analysis Method) [30, 31]:
 - $MEHARI = [Riesgo (Amenaza, Activo) = Probabilidad (Amenaza) * Vulnerabilidad (Amenaza, Activo) * Impacto (Amenaza, Activo)]$
- OCTAVE (The Operationally Critical Threat, Asset, and Vulnerability Evaluation) [32]:
 - $OCTAVE = [Riesgo (Amenaza, ActivoCritico) = Impacto (Amenaza, ActivoCritico) * Vulnerabilidad (ActivoCritico)]$
- NIST SP 800-30 (Risk Management Guide for Information Technology Systems) [33]:

- $NIST SP 800-30 = [Riesgo (Amenaza, Activo) = Probabilidad (Amenaza) * Vulnerabilidad (Amenaza, Activo) * Impacto (Amenaza, Activo)]$

- CORAS (Construct a platform for Risk Analysis of Security Critical Systems) [34]:

- $CORAS = [Riesgo (Amenaza, ActivoCritico) = Impacto (Amenaza, ActivoCritico) * Vulnerabilidad (ActivoCritico)]$

En otros casos, estamos investigando cómo añadir algunas variables diferenciadas de las metodologías, como las “necesidades” en el caso de EBIOS, las “ExpectativaPérdidaAnual” de ISAMM, o el concepto de “Incidente” propuesto por IT-Grundschtz y por AS/NZS 4360, que podría encajar en el concepto de “Evento” propuesto por MARISMA:

- EBIOS (Expression of Needs and Identification of Security Objectives) [35]:
 - $EBIOS = [Riesgo (amenaza, activo, necesidades) = Impacto (amenaza, necesidades) * Vulnerabilidad (amenaza, activo)]$
- ISAMM (Information Security Assessment and Monitoring Method) [36]:
 - $ISAMM = [Riesgo (Amenaza, Activo) = ExpectativaPérdidaAnual (Amenaza, Activo) = Probabilidad (Amenaza, Activo) * PromedioPérdida (Amenaza, Activo)]$
- IT-Grundschtz: (IT Baseline Protection Manual) / BSI Standard 100-[2-3]) [37]:
 - $IT-Grundschtz = [Riesgo (Incidente, Activo) = Probabilidad (Incidente) * Consecuencias (Incidente, Activo)]$
- AS/NZS 4360 [38] & ISO31000:2018 [39]:
 - $AS/NZS 4360 = [Riesgo (Incidente, Activo) = Probabilidad (Incidente) * Consecuencias (Incidente, Activo)]$

Por otro lado, una vez que tenemos calculado el nivel de riesgo es importante tener la capacidad de aprender de los eventos, y desarrollar métricas que nos permitan re-alinear el valor subjetivo de los elementos iniciales para ajustarlos a la realidad.

Las métricas que forman parte de este apartado son:

- Métricas asociadas al Valor de Amenaza – Probabilidad de Ocurrencia:
 - Valor Actual Recomendado para la Probabilidad de Ocurrencia de la Amenaza - Recommended Actual Value for the Probability of Occurrence of the Threat (RAVPOT): Mediante un evento de seguridad podemos determinar si el valor actual de la

probabilidad de ocurrencia de una amenaza es correcto, o debería re-alinearse.

Para ello lo primero que haremos será considerar establecer rangos de valor para esa variable (Ej: en el caso de MARISMA será “1 día” la unidad base). De esta forma, si consideramos que la probabilidad de ocurrencia de una amenaza es “Alta si ocurre varias veces al mes” y “Muy Alta si ocurre varias veces al día”, e inicialmente la tenemos configurada como “Alta”, y tenemos notificados varios eventos relacionados con esa amenaza en un día, el sistema podrá recomendar el cambio de valor.

- *RAVPOT = Ante un Evento => Recalcular la probabilidad de ocurrencia en jornadas y compararla con los niveles definidos en los rangos*
 - ⇒ *Si el Rango es diferente al actual sugerir un cambio de nivel.*
 - ⇒ *Sino finalizar*

El conjunto de métricas presentado en este apartado es un conjunto inicial que se irá complementando con el tiempo según evolucione la metodología.

C. Métricas asociadas al GSS.

El Escudo de Seguridad Global (GSS) es un concepto que pretende unificar el poder de agregación de las redes colaborativas para informar a las instancias del riesgo temporal en cada momento sobre diferentes elementos.

Dicho de otra forma, pretendemos que un evento de seguridad que impacte sobre una compañía, pueda ser utilizado para que otras compañías que utilizan ese mismo patrón aumenten sus niveles de protección, generando un escudo de seguridad entre todas las compañías.

Para ello, inicialmente se tienen que definir una serie de dimensiones temporales y geográficas sobre las que calcularemos los datos agregados de las diferentes instancias. Inicialmente se han determinado los siguientes valores:

- *Rangos Temporales:* MuyCorto = Diario, Corto = Semanal, Medio = Mensual, Largo = Trimestral, MuyLargo=Anual.
- *Rangos Geograficos:* Continente, País, Región.

También se han definido un conjunto de métricas que estarán asociadas con cada uno de los principales elementos del Análisis de Riesgos:

- *Control:*
 - *Media del Riesgo Temporal y Externo asociado al Control - Average of the*

Temporary and External Risk associated to the Control (ATERAC).

- *ATERAC = N° de Eventos que ha incluido el control por ud Tiempo (Rangos) x Gravedad del Evento (leve o grave).*
- *Nivel Medio de Implementación del Control - Average Level of Implementation of the Control (ALIC).*
 - *ALIC= Nivel de cobertura media de los controles por ud Tiempo.*
- *Activos:*
 - *Media del Riesgo Temporal y Externo asociado al Tipo de Activo - Average of Temporary and External Risk associated with the Type of Asset (ATERATA).*
 - *ATERATA = N° de Eventos que han incluido el Tipo de Activo por ud Tiempo (Rangos) x Gravedad del Evento (leve o grave).*
 - *Valor medio de los Tipos de Activos - Average value of the Types of Assets (AVTA).*
 - *AVTA = Valor medio de los T.Activo por ud Tiempo.*
- *Amenazas:*
 - *Media del Riesgo Temporal y Externo asociado a la Amenaza - Average of Temporary and External Risk associated with the Threat (ATERAT)*
 - *ATERAT = N° de Eventos que han incluido la Amenaza por ud Tiempo (Rangos) x Gravedad del Evento (leve o grave).*
 - *Media de la Probabilidad de ocurrencia de la Amenaza - Average Probability of occurrence of the threat (APOT).*
 - *APOT = Valor medio de la Probabilidad de Ocurrencia de la Amenaza por ud Tiempo (Rangos).*
 - *Media de la Degradación del Valor Asociado a la Amenaza - Average Degradation of Value Associated with the Threat (ADVAT)*
 - *ADVAT = Valor medio del % de Degradación por ud Tiempo (Rangos).*

Cada evento de seguridad provocará una serie de cambios dinámicos tanto en su propio Análisis de Riesgos, como asociados al patrón del que fue generado. Este proceso se inicia, con la actualización de los valores asociados con su patrón, y éste a la vez provocará en cascada la actualización de todas sus dependencias. El valor cambiará la visión de cada

una de las tablas y se transmitirá a todas las instancias involucradas.

D. Métricas asociadas a Sondas.

Finalmente, se ha considera que es de gran interés poder asociar los patrones, y en concreto elementos como los “Controles”, con herramientas externas que complementen a los “Eventos Manuales” (Incidentes de seguridad reflejados por los usuarios del Sistema de Información), mediante revisiones automatizadas de vulnerabilidades en activos.

Para ello se está trabajando en métricas que permitan establecer esas relaciones de forma automatizada, permitiendo el alineamiento entre estándares (Ej: ISO27001) y los sistemas clásicos de análisis de vulnerabilidades (Ej: Vulnerabilidades BBDD CVE).

Por ejemplo, imaginemos que deseamos generar la capacidad de que un activo de tipo “Software” (SW, según el catálogo de MAGERIT) incluido dentro del alcance de nuestro análisis de riesgos, para un patrón basado en la ISO27001, adquiera la capacidad de monitorizar periódicamente si dicho activo está seguro o no con respecto a un conjunto de nuevas vulnerabilidades.

Actualmente las empresas, incluso las grandes, resuelven este problema de una forma “artesanal”. De esta forma, suelen indicar manualmente a un tercero (Ej: CNPIC) las tecnologías utilizadas en un software de valor para ellos, y este tercero de confianza les reporta mensualmente informe en el que indica si han aparecido nuevas vulnerabilidades relacionadas con dicho software. Una vez revisada, se debe buscar el nivel de riesgo de cada vulnerabilidad y determinar si les puede impactar o no. Dicho proceso está asimismo totalmente aislado del Análisis de riesgos, por lo que aunque existe un cambio en el riesgo asociado a dicho activo, no se traslada al informe de riesgos. De igual forma, el riesgo estará activo durante una ventana de tiempo que puede llegar incluso al mes de duración, algo que no es aceptable en la mayor parte de los casos.

El planteamiento de la metodología MARISMA parte de la creación de un “motor de sondas” que permita conectar los elementos base del patrón, con los elementos externos asociados a las sondas. Por ejemplo, en la Figura 4 podemos ver cómo:

- Por un lado, tomando de referencia el Patrón para Gestión de la Seguridad bajo la normativa de la ISO27001 podemos relacionar un Tipo de Activo del catálogo de MAGERIT (que sería el [SW] – Software) con la familia de amenazas [A] – Ataques Intencionados, y se podría considerar que afectaría al nivel de cumplimiento del control “A.12.2.1 – Controles contra el software malicioso”, disminuyendo el nivel de cobertura de este control ante la aparición de nuevas vulnerabilidades en activos software.
- Por otro lado, la sonda se nutre de la BBDD de vulnerabilidades CVE (Common Vulnerabilities and

Exposures) y de la métrica CVSS (Common Vulnerability Score System) que determina el nivel de gravedad de la vulnerabilidad, de tal forma que se penalizará más o menos el nivel de cobertura del control dependiendo del valor de CVSS. Finalmente, integraremos un extractor de tecnología como BuiltWith que permitirá que, dada una página web o un software en la nube, automáticamente extraerá las tecnologías utilizadas para su desarrollo y las versiones de éstas.

Estas herramientas no siempre nos permitirán automatizar el 100% del análisis de vulnerabilidades, pero reducen de forma considerable el trabajo necesario para controlar la aparición de nuevas vulnerabilidades vinculadas a los activos software, y permiten de forma automática cambiar el nivel de riesgo asociado a los activos de información, permitiendo tomar decisiones sobre cómo afrontar este nuevo riesgo de una forma ágil.

Figura - 4. Ejemplo de sonda

E. Métricas asociadas a la Valoración de Activos.

Uno de los grandes problemas cuando intentamos valorar el riesgo asociado a los activos de información de una compañía es ser capaces de encontrar mecanismos para calcular el valor monetario de estos de la forma más objetiva y precisa posible, dado que este valor es de vital importancia para estimar las pérdidas potenciales debidas a impactos de

seguridad sobre dichos activos.

Dentro de los mecanismos de valoración de activos podemos destacar el método propuesto por Thomas A. Stewart [40] que, en su artículo "Trying to grasp the intangible", propone una metodología ideada por la empresa norteamericana NCI y orientada a medir el valor de los "activos intangibles" de una empresa, que incluirían no sólo la parte de activos TIC (software, claves criptográficas, etc.), sino también otros activos de valor (know-how, valor de la marca, patentes, conocimiento de los mercados, etc.). De esta forma, el método ofrece una orientación sobre cómo medir el valor de los activos en información de una organización.

El método propuesto está formado por siete partes:

1. Paso 1 - Se toma el promedio durante los tres últimos años del beneficio antes de impuestos.
2. A partir del balance de la empresa se toma el promedio, en el mismo período, del valor de los activos tangibles.
3. Se dividen los beneficios del punto 1 por el valor de los activos tangibles del punto 2, y se pasa a %, obteniéndose así el rendimiento sobre activos (ROA).
4. Para el mismo período, se calcula el promedio del ROA para las empresas del sector de la compañía considerada. Si el valor del ROA de una empresa es inferior al ROA promedio del sector, el método deja de aplicarse.
5. Se calcula lo que debería haber ganado la empresa (beneficios antes de impuestos) si hubiera tenido un ROA como el promedio del sector. Esta cantidad es el "exceso" de beneficio que ha tenido respecto a las empresas del sector, y que no se debe (si se ha seguido el razonamiento del método) a los activos tangibles.
6. Se deducen los impuestos, para determinar el "exceso" de beneficios después de impuestos.
7. Finalmente, se calcula cuánto debería tener la empresa en capital para que generara esta cantidad como réditos. Eso nos permitirá obtener un valor global de los activos intangibles de la compañía.

Aunque el método tiene sus ventajas presenta algunas desventajas, como que sólo permite obtener una estimación de un valor global de los activos intangibles de la empresa, pero no su valor individualizado, y por otro lado es difícil de aplicar en PYMES. Aun así, consideramos que puede ser de interés su aplicación en ciertos casos.

Por otro lado, es importante tener en cuenta qué tipos de activos vamos a tener dentro de la compañía, y cómo se podría llegar a valorar cada uno de ellos. Para realizar una primera aproximación a la valoración de los activos utilizaremos el catálogo de activos de MAGERIT [11]:

- *[D] Datos / Información:* Los datos son el corazón que permite a una organización prestar sus servicios.

Este es uno de los tipos de activos más difíciles de cuantificar dentro de una compañía, y requiere de un estudio profundo de investigación que queda fuera del alcance de este artículo, por lo que nos limitaremos a plantar algunas fórmulas sencillas de valoración:

- *Formula1:* La utilizaremos para valorar los ficheros y los datos de BBDD de valor en la compañía, entendiendo que estos hayan sido obtenidos de forma de legal y, por lo tanto, sean declarables por la misma. El cálculo se puede realizar teniendo en cuenta el % de beneficio asociado a esa BBDD (estimado por el departamento contable de la compañía), el número de registros de esa BBDD y aplicando un factor de amortización del 10% según la antigüedad de los datos, ya que cuanto más antiguos sean los datos mayor riesgo existe de que hayan perdido valor de confidencialidad o de generación de conocimiento.

$$\begin{aligned} \text{Valor Activo} &= [\% \text{ BeneficioAsociadoBBDD}] * \\ &[\text{DepreciaciónAsociadaPorRegistro}] \end{aligned}$$

- *Formula2:* Asociada a código fuente desarrollado internamente. Trataremos de dar un precio a un software desarrollado internamente asociándolo al número de horas que se han invertido, por el coste hora, teniendo en cuenta que un 20% del esfuerzo anual se amortiza por depreciación tecnológica. Igualmente, debemos ejercer un factor correctivo según el porcentaje del activo asociado a los beneficios de la compañía (Ej: Un software que se ha desarrollado en tres años con un coste hora de 25€, y un inversión en horas cada año de [100,50,80], tendrá un valor de 3.680 € el tercer año, y si está asociado al 20% del beneficio de la compañía tendrá un valor final de 4.416 €).

$$\begin{aligned} \text{Valor Activo} &= [\text{N}^\circ \text{ Horas Invertidas} \\ &\text{Desarrollo}] * [\text{Coste Hora}] * [\% \\ &\text{DepreciaciónTecnologica}] * [\% \\ &\text{AsociadoBeneficios}] \end{aligned}$$

Existen otras fórmulas que podemos implementar para este tipo de activos (Ej: $[\text{Valor Sector}] * [\text{N}^\circ \text{ Registros Activo}]$, $[\text{Valor Global de Intangibles de la compañía}] - [\text{Valor del Resto de Activos Intangibles menos datos}]$), que podrían obtenerse a partir de preguntas del tipo “¿Sector al que

pertenece la compañía?”, “¿Número de registros del activo? (Ej: proveedores, clientes, ...)”, etc.

Otras características que se podrían valorar para realizar estos cálculos son: i) Calidad de los datos; ii) Si se tienen registrados y documentados legalmente (LOPD); iii) Número de consultas por mes realizadas; iv) % de la facturación de la compañía asociado con ellos; v) Número de empleados que lo utilizan; vi) Número de horas que se usan esos ficheros al año; vii) Antigüedad media de los datos; viii) Naturaleza del dato (Público, privado, confidencial).

- *[K] Claves criptográficas:* La criptografía se emplea para proteger el secreto o autenticar a las partes. Podemos considerar que el valor de una clave está vinculada al valor de la información que protege, o de los beneficios asociados a la misma.

- *Formula1:* Valor asociado a la información que protege.

- *[S] Servicios:* Función que satisface una necesidad de los usuarios (del servicio). El valor de un servicio está directamente asociado al % Beneficios que genera en la compañía, y se puede regir por principios contables.

- *Formula1:* % Beneficios asociados al servicio.

- *[SW] Software - Aplicaciones informáticas:* El valor de un software desarrollado por terceros, o con licencia comercial, se puede regir por principios contables, y en el caso de un código desarrollado internamente por la formula desarrollada en el apartado “[D] – Datos”.

- *[HW] Equipamiento informático (hardware):* Dícese de los medios materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización, siendo pues depositarios temporales o permanentes de los datos, soporte de ejecución de las aplicaciones informáticas o responsables del procesado o la transmisión de datos.

- *Formula1:* Podemos calcular su valor por principios contables: Coste * Amortización.

- *[COM] Redes de comunicaciones:* Incluyen tanto instalaciones dedicadas como servicios de comunicaciones contratados a terceros; pero siempre centrándose en que son medios de transporte que llevan datos de un sitio a otro.

- *Formula1:* Podemos calcular su valor por principios contables: Coste * Amortización.

- *[L] Instalaciones:* En este epígrafe entran los lugares donde se hospedan los sistemas de información y comunicaciones.

- *Formula1:* Podemos calcular su valor por principios contables: Coste * Amortización.

- *[P] Personal:* En este epígrafe aparecen las personas relacionadas con los sistemas de información. En este caso el coste se puede calcular teniendo en cuenta el KnowHow de esa persona asociado al beneficio de la compañía, y con un máximo de antigüedad de 10 años, dado que los conocimientos superiores a 10 años rara vez son útiles en la tecnología.

- *Formula1:* En este caso, el coste se puede calcular teniendo en cuenta el KnowHow de esa persona asociado al beneficio de la compañía, y con un máximo de antigüedad de 10 años, y multiplicado por el salario medio del perfil que tendría que ser reemplazado.

$$\begin{array}{lcl} \text{Valor} & \text{Activo} & = \\ \text{[SalarioMedioPerfil]} & * & \text{[%} \\ \text{BeneficioAsociadoRRHH]} & & \text{*} \\ \text{[FactorCorrectorNumeroAños]} & & \end{array}$$

Este conjunto de métricas debe ser tomado como una base que ira siendo cumplimentada en posteriores investigaciones, según se vaya disponiendo de más casos de uso para su validación.

IV. CONCLUSIONES.

En este artículo se ha analizado el conjunto de métricas e indicadores que se ha desarrollado como parte de la metodología MARISMA para dotar de capacidad de dinamismo y aprendizaje a los análisis de riesgos.

Se han introducido conceptos como el riesgo asociativo entre compañías, que permite que los eventos de seguridad de una compañía puedan ser utilizados por otras compañías para aumentar su nivel de protección.

El conjunto de métricas presentado en el artículo ha sido implementado dentro de la herramienta eMARISMA que da soporte a la metodología MARISMA, y está siendo validado en casos reales dentro del entorno de la “Gestión de la Seguridad” utilizando estándares como la ISO27001 y Magerit, así como la Ley 8/2011 de Infraestructuras Críticas.

Como líneas futuras se está complementando el conjunto de métricas, añadiendo nuevas métricas que puedan generar inteligencia en el sistema, y se está desarrollando una versión de la herramienta que permitirá de forma gratuita que los usuarios puedan utilizar las métricas para valorarlas y generar una base de conocimiento común, que permita aumentar el nivel de protección de cada una de las compañías de forma individual, pero utilizando el conocimiento colectivo de todas.

Podemos concluir, por lo tanto, que ahora mismo es muy importante poder disponer de sistemas de análisis de riesgos dinámicos y que permitan compartir riesgos y colaborar entre diferentes empresas, y que las métricas presentadas en este artículo como parte de la metodología MARISMA son una primera aproximación para conseguir ese objetivo.

AGRADECIMIENTOS

Esta investigación ha sido co-financiada por los proyectos *GENESIS - Security Government of Big Data and Cyber Physics Systems ((SBPLY/17/180501/000202)* financiado por el “JCCM- Consejería de Educación, Cultura y Deportes, y Fondos FEDER”, del proyecto *ECLIPSE – Enhancing Data Quality and Security for Improving Business Processes and Strategic Decisions in Cyber Physical Systems (RTI2018-094283-B-C31)* financiado por la “Ministerio Economía, Industria y Competitividad y fondos FEDER”, y ha contado con el apoyo de las empresas Marisma Shield S.L (www.emarisma.com) y Sicaman Nuevas Tecnologías (www.sicaman-nt.com).

REFERENCIAS

- [1] Huerta, M., et al. *Design of a building security system in a university campus using RFID technology*. in *2017 IEEE 37th Central America and Panama Convention (CONCAPAN XXXVII)*. 2017. IEEE.
- [2] Le Grand, G. and E. Adar. *White cyber knight—a Risk Assessment tool for network resilience evaluation*. in *the proceedings of the International Workshop on Complex Network and Infrastructure Protection (CNIP'06), Rome*. 2006.
- [3] Vivas, T., A. Zambrano, and M. Huerta. *Mechanisms of security based on digital certificates applied in a telemedicine network*. in *2008 30th Annual International Conference of the IEEE Engineering in Medicine and Biology Society*. 2008. IEEE.
- [4] Huerta, M., et al. *Implementation of a open source security software platform in a telemedicine network*. in *Proceedings of the 9th WSEAS international conference on Advances in e-activities, information security and privacy*. 2010. World Scientific and Engineering Academy and Society (WSEAS).
- [5] Pirrone, J. and M. Huerta. *Security Mechanism for Medical Record Exchange Using Hippocratic Protocol*. in *World Congress on Medical Physics and Biomedical Engineering 2018*. 2019. Springer.
- [6] Eloff, J. and M. Eloff, *Information Security Management - A New Paradigm*. Annual research conference of the South African institute of computer scientists and information technologists on Enablement through technology SAICSIT'03, 2003: p. 130-136.
- [7] Steve, E., *An Introduction to information systems risk management*. SANS Institute InfoSec Reading Room. Available on-line at http://www.sans.org/reading_room/whitepapers/auditing/introduction-information-system-risk-management_1204. Accessed March, 2006. **16**: p. 2011.
- [8] Bača, M. and F. Varaždin, *The risk assessment of information system security*. Fakultet organizacije i informatike, Sveučilište u Zagrebu. < dostupno na http://cuc.carnet.hr/cuc2004/program/radovi/a5_baca/a5_full.pdf>, [očitano 07.10. 2010], 2004.
- [9] Restrepo, L.O. and F.J.V. Duque, *Gestión de riesgos en eTOM. Un análisis comparativo con los estándares de riesgo corporativo*. Revista Logos, Ciencia & Tecnología, 2017. **9**(1): p. 85-99.
- [10] Ortiz Restrepo, L., V. Duque, and F. Javier, *Gestión de riesgos en eTOM. Un análisis comparativo con los estándares de riesgo corporativo*. Revista Logos Ciencia & Tecnología, 2017. **9**(1): p. 85-99.
- [11] Magerit V3, *Methodology for Information Systems Risk Analysis and Management*, in *Ministerio de Hacienda y Administraciones Públicas* 2012: Spain.
- [12] Wangen, G., *Information security risk assessment: a method comparison*. Computer, 2017. **50**(4): p. 52-61.
- [13] Fakrane, C. and B. Regragui. *Interactions and Comparison of It Risk Analysis Methods*. in *2018 4th International Conference on Cloud Computing Technologies and Applications (Cloudtech)*. 2018. IEEE.
- [14] Jeannot, F., *Méthodologies d'évaluation et gestion de risques en sécurité*. Montréal, Canada, Mai 2018, R518, v1.0. 2018.
- [15] Benavides Sepúlveda, A.M. and C.A. Blandón Jaramillo, *Modelo de sistema de gestión de seguridad de la información basado en la norma NTC ISO/IEC 27001 para instituciones públicas de educación básica de la comuna Universidad de la ciudad de Pereira Alejandra*. 2017.
- [16] Bommman, W.G., *Information security risk management: a holistic framework*, 2004, University of Johannesburg.
- [17] Refsdal, A., B. Solhaug, and K. Stølen, *Cyber-risk management*, in *Cyber-Risk Management* 2015, Springer. p. 33-47.
- [18] Zudin, R., *Analysis of information risk management methods*. University of Jyväskylä, 2014.
- [19] Carrillo Sánchez, J.P., *Guía y análisis de gestión de riesgos en la adquisición e implantación de equipamiento y servicios de tecnologías de información y comunicaciones para proyectos de alcance nacional*, 2012, Quito: EPN, 2012.
- [20] Pacheco Pozo, D.C., *Propuesta de un plan de contingencia de TI para la empresa LOGICIEL*, 2016, Quito, 2016.
- [21] Dehkhoda, D., *Combining IRAM2 with Cost-Benefit Analysis for Risk Management: Creating a hybrid method with traditional and economic aspects*, 2018: Department of Computer Science, Electrical and Space Engineering, Luleå University of Technology.
- [22] Wangen, G. *An initial insight into information security risk assessment practices*. in *2016 Federated Conference on Computer Science and Information Systems (FedCSIS)*. 2016. IEEE.
- [23] Pandey, S. and K. Mustafa, *Risk Assessment Framework (RAF)*. International Journal of Advanced Research in Computer Science, 2010. **1**(3).
- [24] López, D., O. Pastor, and L.J.G. Villalba, *Concepto y Enfoques sobre el Análisis y la Gestión Dinámica del Riesgo en Sistemas de Información*. Actas de la XII Reunión Española de Criptología y Seguridad de la Información (RECSI 2012), Donostia-San Sebastián, España, 2012.
- [25] Saripalli, P. and B. Walters. *Quirc: A quantitative impact and risk assessment framework for cloud security*. in *2010 IEEE 3rd international conference on cloud computing*. 2010. IEEE.
- [26] Li, S., et al., *An improved information security risk assessments method for cyber-physical-social computing and networking*. IEEE Access, 2018. **6**: p. 10311-10319.
- [27] Sicari, S., et al., *A risk assessment methodology for the Internet of Things*. Computer Communications, 2018. **129**: p. 67-79.
- [28] CRAMM. *Siemens Enterprise Communications Ltd. "CRAMM toolkit"*. 2009; Available from: <http://www.cramm.com/>.
- [29] CESG, S.S.a., *CRAMM User Guide*, 2005: Security Service and CESG (UK Government).
- [30] MEHARI, *MEHARI. Risk analysis and treatment Guide*, C.d.I.S.d.I.I. Français, Editor 2010.
- [31] MEHARI, *MEHARI. Overview*, C.d.I.S.d.I.I. Français, Editor 2019.
- [32] OCTAVE. *CERT – Software Engineering Institute, Carnegie Mellon*. 2009; Available from: <http://www.cert.org/octave/>.
- [33] NIST SP 800-30 Rev.1, *NIST SP 800-30 Rev. 1. Guide for Conducting Risk Assessments*, N.I.o.S.a.T. (NIST), Editor 2012, Sep 2012.
- [34] Bjørn, A. *CORAS, A Platform for Risk Analysis on Security Critical Systems—Model-based Risk Analysis Targeting Security*. 2002. EWICS Symposium.
- [35] de la Défense Nationale, S.G., *EBIOS-Expression des Besoins et Identification des Objectifs de Sécurité, Méthode de Gestion des risques*, 2010.
- [36] Telindus, *ISAMM - Information Security Assessment & Monitoring Method*, 2002.
- [37] BSI_S100-2, *BSI-Standard 100-2. IT-Grundschutz Methodology*, F.O.f.I.S. Germany., Editor 2008.
- [38] AS/NZS 4360:2004, *Standards Australia and Standards New Zealand, in Risk Management* 2004, Standards Association Melbourne Info Center: Sydney, NSW.
- [39] ISO_31000:2018, *ISO 31000:2018. Risk Management - Guidelines*, 2018, ISO/TC 262 Risk management: International Organization for Standardization. p. 16.
- [40] Stewart, T.A., *Trying to grasp the intangible*. Fortune, October, 1995. **2**(1995): p. 91-93.

Luis Enrique Sánchez es Doctor y Máster en Informática y es profesor asociado de la Universidad de Castilla-La Mancha (Ciudad Real, España), Master en Auditoría de Sistemas de Información por la Universidad Politécnica de Madrid, y Auditor Certificado de Sistemas de Información por ISACA. Es Director de los departamentos de Servicios Profesionales y de I+D de la empresa Sicaman Nuevas Tecnologías S.L. Sus actividades de investigación son sistemas de seguridad de gestión, métricas de seguridad, minería de datos, limpieza de datos e inteligencia de negocios. Participa en el grupo de investigación GSyA del departamento de sistemas de información y tecnologías de la Universidad de Castilla-La Mancha, en Ciudad Real (España). Su correo electrónico es luisenrique@sanchezcrespo.org.

Antonio Santos-Olmo es Licenciado en Informática y es profesor asociado de la Escuela Superior de Informática de la Universidad de Castilla-La Mancha en Ciudad Real (España), Master en Auditoría de Sistemas de Información por la Universidad Politécnica de Madrid, y Auditor Certificado de Sistemas de Información por ISACA. Es Director de los departamentos de Software Factory de la empresa Sicaman Nuevas Tecnologías S.L. Sus actividades de investigación son sistemas de seguridad de gestión, métricas de seguridad, minería de datos, limpieza de datos e inteligencia de negocio. Participa en el grupo de investigación GSyA del Departamento de de sistemas de información y tecnologías de la Universidad de Castilla-La Mancha, en Ciudad Real (España). Su correo electrónico es asolmo@sicaman-nt.com.

Julio Moreno es Máster y estudiante de doctorado en Informática por la Universidad de Castilla-La Mancha. Su investigación se centra en la seguridad y privacidad de los datos, así como en la creación de un marco de gobierno para Big Data. Es miembro del grupo de investigación GSyA del departamento de sistemas de información y tecnologías de la Universidad de Castilla-La Mancha. Su correo electrónico es julio.moreno@uclm.es.

Manuel A. Serrano es Máster y doctor en Informática por la Universidad de Castilla-La Mancha. Es profesor titular en la Escuela Superior de Informática de la Universidad de Castilla-La Mancha en Ciudad Real. Su investigación se centra en la calidad de software de los datos, la medición de software y la calidad y medición de almacenes de datos y Big Data. Su correo electrónico es manuel.serrano@uclm.es.

David G. Rosado tiene un Máster y es doctor en Informática por la Universidad de Málaga y por la Universidad de Castilla-La Mancha, respectivamente. Es profesor titular en la Escuela Superior de Informática de la Universidad de Castilla-La Mancha en Ciudad Real. Su actividad investigadora se centra en seguridad de sistemas de información, Cloud Computing y Big Data. Sobre estos temas, él ha publicado numerosos artículos en conderencias de ámbito nacional e internacional, también es editor y coeditor de varios libros. Es autor de varias publicaciones en revistas nacionales e internacionales (Information Software Technology, System Architecture, Network and Computer Applications, etc.). Él es miembro del comité de programa de numerosas conferencias y workshops nacionales e internacionales. Es miembro del grupo de investigación GSyA del departamento de sistemas de información y tecnologías de la Universidad de Castilla-La Mancha. Su correo electrónico es david.grosado@uclm.es.

Eduardo Fernández-Medina es Máster y doctor en Informática por la Universidad de Castilla-La Mancha. Es profesor catedrático en la Escuela Superior de Informática de la Universidad de Castilla-La Mancha en Ciudad Real (España). Su actividad investigadora se centra en el campo de la seguridad de sistemas de información, en particular en seguridad en Big Data, Cloud Computing y sistemas ciberfísicos. En estas temáticas, él es coeditor de varios libros y capítulos de libros, y ha publicado numerosos artículos en conferencias nacionales e internacionales (BPM, UML, ER, ESORICS, TRUSTBUS, etc.). Es autor de más de cincuenta publicaciones en revistas internacionales (Decision Support Systems, Information Systems, ACM Sigmod Record, Information Software Technology, Computer & Security, Computer Standards and Interfaces, etc.). Él lidera el grupo de investigación GSyA del departamento de sistemas de información y tecnologías de la Universidad de Castilla-La Mancha y pertenece a varias asociaciones profesionales y de investigación (ATI, AEC, AENOR, etc.). Su correo electrónico es eduardo.fdezmedina@uclm.es.