Concepto y Enfoques sobre el Análisis y la Gestión Dinámica del Riesgo en Sistemas de Información

David López[1,2], Oscar Pastor[2], Luis Javier García Villalba[1]

[1] Grupo de Análisis, Seguridad y Sistemas (GASS)
Dto. de Ingeniería del Software e Inteligencia Artificial (DISIA)
Facultad de Informática, Despacho 431
Universidad Complutense de Madrid (UCM)
Calle Profesor José García Santesmases s/n
Ciudad Universitaria, 28040 Madrid
Email: {dlcuenca, javiergv@fdi.ucm.es}

[2] Ingeniería de Sistemas para la Defensa de España S.A. (ISDEFE)
Dir. Defensa y Seguridad
Email: {dlcuenca, opastor@isdefe.es}

***Abstract*—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, cuyo principio es la actualización incesante de los parámetros que intervienen en el cálculo del riesgo para la optimización de su tratamiento posterior. Finalmente, se proponen las posibles tendencias futuras para la mejora en este ámbito.**

I. Introducción

La Gestión del Riesgo (en adelante GR) persigue lograr un conocimiento lo más realista posible de aquellas circunstancias que podrían afectar a los procesos o servicios, causando daños o pérdidas, de modo que se puedan establecer prioridades y asignar requisitos de seguridad para afrontar convenientemente dichas situaciones. Estos riesgos que pueden ser de muy diferente naturaleza, cobran especial importancia cuando afectan al ámbito de las tecnologías de la información, debido a su imbricación en gran cantidad de los servicios que regulan nuestra sociedad actual.

Con este fin, la GR se apoya en el Análisis de Riesgos (en adelante AARR), que conforme a [1] es el proceso para identificar, estudiar y evaluar a través de las diferentes variables implicadas, potenciales eventos que afecten a los objetivos de una organización y sus consecuencias. Para ello, realiza una predicción del futuro, basada en el pasado histórico y el análisis cuidadoso de los eventos, como recoge el Capítulo II. En el Capítulo III se presentan los conceptos de Análisis y Gestión Dinámica de Riesgos, así como las tendencias actuales en dichos ámbitos, recapitulándose finalmente en el Capítulo IV las conclusiones extraídas y las propuestas a desarrollar.

II. Conceptos sobre Análisis y Gestión de Riesgos en Sistemas de la Información

El proceso de AARR comprende un ejercicio de comprensión, catalogación y valoración de aspectos que adquieren gradualmente una complejidad sustancial. Un AARR de utilidad para a la GR debe ser riguroso y permitir ser contrastado y comparado objetivamente. De otro modo se podría inducir un sesgo, que condicione las decisiones basadas en los resultados del AARR afectando a su fiabilidad y efectividad. Por ello se persigue una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista. En el campo de las Tecnologías de Información, destacan las metodologías de AARR y GR mostradas a continuación, fundamentalmente patrocinadas por los organismos mencionados:

- ISO 27005:2008 (IEC - Internacional) [2].
- UNE 71504:2008 (AENOR - España) [3].
- MAGERIT (Ministerio AAPP - España) [4].
- OCTAVE (SEI Carnegie Mellon University - USA) [5].
- CRAMM (Siemens Insight Consulting - UK) [6].
- EBIOS (DCSSI - Francia) [7].
- IT Baseline Protection Manual (BSI - Alemania) [8].
- NIST SP800-30 (NIST - USA) [9].

La European Network and Information Security Agency (ENISA) publica un catálogo [10] de las metodologías de Análisis y Gestión de Riesgo con mayor reconocimiento internacional, así como de las herramientas de qué se dispone para su aplicación, y que aportan una base de conocimiento, flujos de trabajo y automatización de cálculos. Estas metodologías giran en torno a conceptos similares, como los recogidos de manera genérica en [2] y que quedan plasmados[1] en la Fig. 1.

- Activos: Elementos con valor, fundamentalmente Hardware, Redes y Software, pero también los relacionados,

[1]Basado en el concepto ilustrado para la metodología Magerit en la web del CNI:https://www.ccn-cert.cni.es/publico/herramientas/pilar43/index.html

como el personal (administradores, usuarios, etc.), infraestructuras (edificios o suministros) u otros intangibles como la propia información, la imagen o la reputación.
- Amenazas: son los eventos o causas que pueden desencadenar un incidente en la Organización, produciendo daños materiales o pérdidas inmateriales, al afectar en alguna medida a los activos de ésta.
- Vulnerabilidades: Defecto o debilidad en los procedimientos, diseños, implementaciones o controles internos de seguridad de los sistemas que pueden ser explotados (accidental o intencionadamente).
- Impacto: Resultado de que una amenaza se materialice sobre un activo, sacando provecho de una vulnerabilidad asociada a éste, y provocándole una determinada degradación o pérdida de valor.
- Frecuencia/Probabilidad: La probabilidad es un indicador de posibilidad, que determina si una potencial vulnerabilidad puede ser explotada a través del entorno de amenaza apropiado, mientras que en el caso de la frecuencia el indicador refleja el número de veces que se materializaría la amenaza por unidad de tiempo.
- Riesgo (residual): Grado de exposición a que una amenaza se materialice sobre uno o más activos, causando daños a una Organización. Tras aplicar salvaguardas al sistema, debería reducirse hasta un riesgo residual.
- Salvaguardas: Medidas de seguridad, procedimientos o mecanismos tecnológicos orientados a reducir el riesgo.

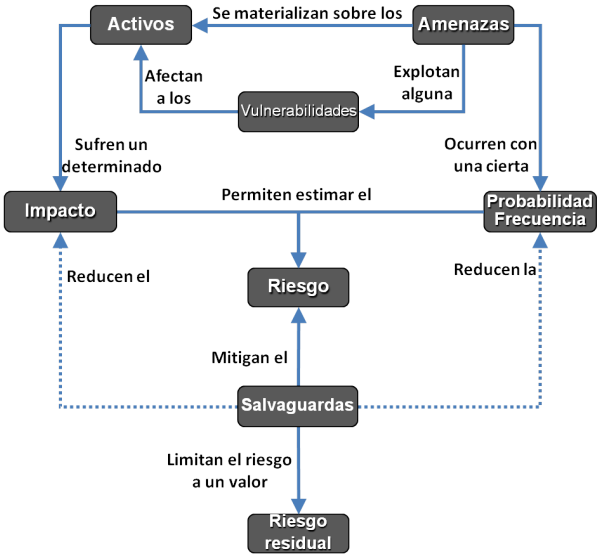

Fig. 1. Diagrama de conceptos genéricos implicados en el AARR

III. El Análisis y la Gestión de Riesgos Dinámica

La introducción de cambios en los sistemas de información, altera en mayor o menor medida su situación de partida, y por tanto la base del cálculo del riesgo sobre el que trabaja un AARR clásico. El factor de incertidumbre que aparece tras estas alteraciones continuas del sistema y de su entorno hace que la fiabilidad de los AARR y con ello las conclusiones asociadas, pierdan valor conforme transcurre el tiempo. Una adecuada GR contemplaría esta evolución por medio de un proceso reiterativo de análisis y tratamiento del riesgo, con la intención de paliar las desviaciones sobre el modelo de sistema de la información de partida. Tal es el caso del estándar internacional ISO 27001 [11] que adapta el concepto de ciclo PDCA (Plan-Do-Check-Act) a los Sistemas de Gestión de Seguridad en la Información o SGSI, estableciendo la obligatoriedad de una revisión periódica del AARR y de una actualización de los planes para mitigar los riesgos detectados. En el caso del NIST (National Institute of Standards and Technology) contempla 6 pasos dentro del proceso de GR, que se repiten a lo largo del ciclo de vida del sistema [12]. Sin embargo, esta es una falsa percepción de dinamismo ya que la repetición del proceso tiene lugar en intervalos discretos de tiempo y, por pequeños que éstos sean, hay margen para la ocurrencia de cambios que afecten de forma inmediata y crucial al riesgo.

A. El Concepto de Análisis y Gestión Dinámica del Riesgo

Ante la posibilidad de eventos o cambios sobrevenidos a los sistemas de información o a su entorno, en el lapso transcurrido entre diferentes iteraciones de un AARR, surge la necesidad de contemplar una forma de adaptarse de manera continua a las variaciones que afectan al resultado de un AARR. Esto permitiría actualizar las conclusiones asociadas a éste y por tanto las medidas a implantar para adecuar el proceso de GR.

Son múltiples las variables contempladas, a lo largo de las fases que componen un AARR, que se ven sometidas a una aleatoriedad y dinamismo considerable. éstas se pueden agrupar en 4 grandes conjuntos: Cambios en el sistema por la introducción, alteración o supresión de máquinas, aplicaciones o arquitecturas de red, así como alteraciones en servicios, recursos, mantenimientos, proveedores, etc.; Nuevas vulnerabilidades y amenazas detectadas y en el peor de los casos, desconocidas; Evolución de las amenazas conocidas y monitorizadas por los sistemas de seguridad desplegados, o del nivel de riesgo en el entorno, causado por amenazas expresas o previsión de desastres naturales, entre otras; Aplicación de políticas de seguridad o salvaguardas, que modifiquen el modo en que las amenazas afectan a los activos o la probabilidad de que los riesgos se manifiesten.

Si bien en algún caso puntual se expone que el AARR Dinámico podría ser la simple reiteración del AARR en periodos definidos de tiempo [13], son múltiples los ejemplos, como se mostrará en adelante, que abogan por que el fundamento real de un Sistema de AARR Dinámicos radica en una realimentación continua de los datos de entrada, gracias a los cuales se pueden caracterizar las variables que modelan el riesgo para posteriormente realizar su cálculo. Así, si por cualquiera de las circunstancias recogidas anteriormente ocurre alguna modificación en el sistema, las entradas que alimentan el análisis se verán afectadas en alguna medida y el cálculo del riesgo será susceptible de actualización. A partir de dicha actualización se acometerían las acciones

oportunas dentro de una Gestión Dinámica del Riesgo. Esta realimentación es la que se recoge en [14] (ver Fig. 2).

En la bibliografía analizada, se utilizan ocasionalmente referencias al Online Risk Assessment ([15], [16]) o Real Time Risk Assessment ([12], [17]) como sinónimos del aquí denominado Dynamic Risk Assessment, siendo éste el término más comúnmente utilizado y en ocasiones representado con las siglas DRA. En todos los casos se hace referencia a una actualización del AARR en base a los cambios continuos que sufre el sistema y su entorno, y en ocasiones al correspondiente tratamiento del riesgo con lo que se completaría el flujo del proceso de Gestión Dinámica del Riesgo.

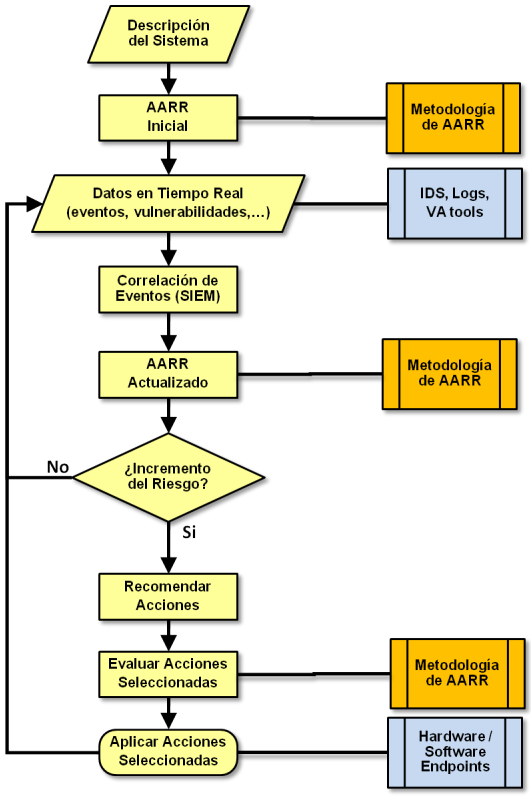

Fig. 2. Flujo de DRA basado en un bucle reiterativo (del original en [14])

B. Evolución del AARR Dinámico

Se ha buscado en primer lugar una catalogación de los diferentes enfoques analizados, en función del ámbito o de los principios que los han inspirado, sin que se disponga de una ontología al efecto. Estos enfoques sobre el AARR Dinámico han convergido en torno a las siguientes temáticas, siendo en ocasiones difícil establecer la línea de separación:

1) ***Alimentación desde BBDD****:* La recopilación masiva de datos objetivos y fidedignos, para la alimentación de los AARR es una de las principales dificultades del proceso, incluso en los modelos estáticos. La idea de obtener esta información a partir de una BBDD como presenta [18] parece una solución apropiada, pero plantea múltiples retos. De un lado, deben seleccionarse fuentes especializadas y fiables (especialmente en el caso de seleccionarse fuentes externas) para cada variable que interviene en el cálculo, y que además estén permanentemente mantenidas en el tiempo. Por otro, deberá recurrirse a formatos estandarizados para el intercambio de dichos datos y su comprensión adecuada [14] tales como CVE, NVD, CPE, OVAL, KML, CVSS, etc.

Actualmente, existirían bases de datos para uso público como la National Vulnerability Database del NIST [19], especializadas fundamentalmente en la publicación de vulnerabilidades en los sistemas informáticos. También se encuentran en número cada vez mayor [20], iniciativas de gobiernos y consorcios para compartir información, anónimamente cuando las circunstancias lo requieren, sobre amenazas, vulnerabilidades, intrusiones o anomalías cibernéticas, a través de entidades como CERTs (Computer Emergency Response Team).

2) ***Grafos y árboles de ataque****:* El razonamiento detrás de los árboles o Grafos de Ataque es semejante. Con sus peculiaridades, Grafos y árboles de Ataque [21], se componen de nodos conectados que representan los pasos que el atacante debe dar en función de la arquitectura de red y sus vulnerabilidades, para alcanzar a un objetivo. Podrían existir múltiples caminos (o ramas) que conduzcan a un mismo objetivo. Cada nodo llevaría asociada una probabilidad de ser superado, de modo que el encadenamiento de probabilidades de los nodos de cada camino proporcionaría la probabilidad de alcanzar el nodo final u objetivo. Esta tipología de AARR, se presta a una Gestión Dinámica del Riesgo basada en la respuesta en tiempo real a incidentes de seguridad, que están teniendo lugar en los SSII. Para ello dependen en primer lugar de la detección temprana (in-fraganti) del incidente, a través de los medios o herramientas oportunos tales como IDS/IPS, que permita conocer en qué punto del árbol o grafo de ataque se encuentra el sistema, para poder reaccionar posteriormente en un intento de evitar o mitigar los efectos adversos del ataque. En este terreno, las herramientas actuales tienden a ofrecer alarmas y valoraciones en base a factores internos, pero no en base a una metodología de AARR reconocida que permita integrar el valor del riesgo, en el contexto global del sistema.

Los cálculos, como ocurre en ([21], [22][2]), se implementan principalmente mediante Redes Bayesianas que permiten representar, a través de un modelo gráfico, las relaciones probabilísticas entre un conjunto de variables en un grafo acíclico dirigido (DAG). En ([23], [24]) se analiza el uso de Hierarchical Coordinated Bayesian Model (HCBM), para analizar la ocurrencia de eventos extremos, integrando múltiples Bases de Datos de conocimiento sobre amenazas. Trabajos como ([25], [26]) plantean que los recorridos y la probabilidad de explotación también pueden ser específicos, en función del perfil del atacante y sus habilidades (script kiddies, hackers, insiders, etc.). Para ello, se establecen diferentes perfiles, a los que se asocian vulnerabilidades que pueden ser explotadas más previsiblemente en base a las supuestas habilidades del

[2]El artículo hace referencia a un enfoque examinado posteriormente, pero que también incluyen el uso de árboles de ataque.

atacante, obteniendo árboles más personalizados, que también se calculan mediante el uso de Redes Bayesianas. Un caso particular es el del modelo NSRM (Network Security Risk Model) aplicado a redes de control de procesos (PCN), que son características de las Infraestructuras Críticas (ICs), conforme a [27]. Si bien caracteriza el concepto de dinamismo en el AARR como un contraste estático de evaluaciones del riesgo obtenidas mediante simulaciones con árboles de ataque en el ámbito cibernético, frente a una evaluación inicial o baseline con el fin de optimizar las diferentes estrategias de mitigación, es autocrítico en este sentido abogando por la necesidad de introducir datos en tiempo real y aprendizaje para responder a las dinámicas de un ataque real.

*3) **Enfoque mixto**:* Las soluciones planteadas se centran en algunos aspectos que afectan al cálculo del riesgo, pero dejan muchos otros fuera de consideración. Conscientes de ello, se han desarrollado plataformas más complejas que buscan un mayor ámbito de cobertura, teniendo en cuenta un rango más diversificado de factores. Es el caso de [22] que se centra en el uso de árboles de ataque, cerrando el ciclo de Gestión de Riesgos al introducir planes de mitigación con optimización de salvaguardas (coste vs utilidad), a la par que saca partido de la BBDD CVSS sobre vulnerabilidades y las métricas sobre explotación asociadas a éstas. Por otro lado contempla la generación de Planes de Mitigación en un momento puntual del tiempo en base a una optimización del ROI (retorno de la inversión, utilizado para establecer una relación coste-beneficio) de las medidas a implantar. Destaca especialmente [14] que se plantea atacar 3 problemas actuales de la gestión de herramientas de seguridad, como son: su escasa interoperabilidad, la difícil visualización de los datos y la falta de visión de conjunto. Para ello conjuga el uso de dos herramientas en desarrollo en el entorno OTAN que se alimentarían mutuamente:

- CIAP (Consolidated Information Assurance Picture) que recopila información en base a múltiples estándares sobre la arquitectura de red, vulnerabilidades y alertas, desde diferentes fuentes.
- DRA (Dynamic Risk Assessment) que realiza AARR casi en tiempo real, utilizando un AARR estático inicial (conjuntamente con árboles de ataque) y después dentro en un bucle continuo, facilitando posibles medidas en respuesta a los riesgos detectados.

*4) **Monitorización del estado del sistema**:* La tendencia actual en gestión de seguridad en SSII es la tecnología SIEM (Security Information and Event Management) [28] que aporta capacidades para la gestión de registros de seguridad (logs), monitorización de redes, gestión de incidentes y generación de informes sobre seguridad. Estas herramientas se basan fundamentalmente en arquitecturas de IDS (Intrusion Detection Systems) e IPS (Intrusion Prevention Systems) que permiten detectar y/o prevenir en tiempo real trazas de actividad maliciosa dirigida contra la red y sus recursos. El conocimiento de dichas actividades detectadas por los IDS/IPS, puede ser utilizado para reevaluar metodológicamente el nivel de riesgo del sistema en tiempo real, teniendo en consideración las nuevas circunstancias temporales que afectan a éste.

Esta aplicación del AARR Dinámico concebida como un indicador a más alto nivel que el de los árboles de Ataque, sería el caso de [16] que presenta un sistema IPS distribuido con capacidad para predecir niveles de amenazas con Hidden Markov Models y estimar riesgos sobre los activos afectados, mediante el uso de lógica difusa. Para ello plantea el uso de una detección descentralizada de amenazas con DIPS (Distributed IPS) que optimice la predicción de las amenazas, infiriendo el riesgo sobre los activos en función del estado determinado para el sistema (Normal, Intento de Intrusión, Intrusión en Progreso o Ataque Exitoso). En la misma línea se mueve el modelo desarrollado en [29]. Los modelos de Markov (HMM) mencionados caracterizan un sistema dinámico en el que la evolución futura depende únicamente de su estado actual, sin importar lo ocurrido en el pasado. En [15] se presenta un modelo (bajo el nombre de IDAM&IRS) que determina cuantitativamente el riesgo existente en un escenario de intrusión, evaluando el estado de seguridad del objetivo. Para ello filtra y correla alertas de IDS, estimando después (por su volumen, relevancia, realismo y tipología) el estado del riesgo para los activos, para finalmente realizar acciones mitigadoras. Se infiere el riesgo mediante un cálculo (D-S evidence theory) basado en evidencias e incógnitas, planteamiento que podría ser considerado semejante al de los HMM.

Existen trabajos en los que se recurre a nociones propias del campo de la biología celular, aplicando el concepto de Autonomic Defense Network (ADN) [30] que se basa en la cooperación de diferentes dispositivos de seguridad y monitorización distribuidos en la red. Con la intención de obtener un enfoque más a alto nivel del AARR, en lugar del enfoque eminentemente técnico que normalmente tienen, en [17] se establece la existencia de diferentes tipos de señales (alarma, discriminación o co-estimulación) intercambiados entre estos dispositivos o centros de análisis, conforme al Danger Model que inspira a las ADN. La combinación de estas señales, disparadas por eventos ocurridos en la red, implican la existencia/materialización de un riesgo real, mientras que la existencia de una sola indica un estado intermedio de riesgo.

El cálculo del riesgo en tiempo real en base a la evolución de determinados indicadores de los SSII, no se limita a la detección de intrusiones, teniendo aplicación en aspectos operativos como la gestión de recursos de los SSII, que podría afectar a la continuidad de los servicios y por tanto al nivel de riesgo del negocio. En [31] se recurre a modelos para una distribución dinámica de los recursos a dedicar a la computación de tareas, en función del riesgo de incumplimiento de SLAs pactados con clientes. El modelo se adapta a incidencias sobrevenidas como caída de nodos o problemas en la planificación y el personal técnico disponible. Para ello se recurre a modelos estadísticos bayesianos para el cálculo y transmisión de probabilidades de fallo de los nodos. Estos modelos operan sobre procesos de Poisson con estimaciones de parámetros basados en distribuciones Gamma (a partir de datos empíricos). En casos como [32] el AARR Dinámico se

aplica a la configuración de redes MANET Ad-Hoc en función del riesgo inherente a sus nodos, en base a parámetros de éstas variables en el tiempo, tales como sobrecargas, pérdidas de paquetes, retrasos, rendimientos, etc. En el ámbito de los sistemas SCADA (Supervisory Control And Data Acquisition) que permiten la monitorización de redes que soportan entre otros, los sistemas de gestión de electricidad (EMS), la gestión en tiempo real del riesgo se ha venido desarrollando desde tiempo atrás. En el caso de [33] esta gestión on-line se aplica desde el punto de vista de la operativa, en relación a caídas de voltaje en redes de distribución eléctrica.

C. Gestión/Tratamiento Dinámico del Riesgo

La ventaja que un AARR Dinámico plantea frente al modelo implantado de análisis estático es la de una gestión también dinámica, del riesgo en tiempo real, que permita su tratamiento respondiendo con las salvaguardas más adecuadas donde se manifieste realmente el riesgo. Del mismo modo que en el proceso de AARR se plantean diferentes enfoques, también en su gestión se perciben diferentes estrategias con versatilidad más dinámica que la de planteamientos más arraigados:

1) ***árboles de decisión para optimización del riesgo****:* Una aplicación alternativa de los árboles en el ámbito de la simulación de riesgos, es su uso para la optimización de las medidas mitigadoras a implementar frente a un cambio en los SSII o de su entorno. En este caso, el árbol no es utilizado para determinar el riesgo en función del nivel de avance del ataque, si no para determinar cuáles serían las medidas más adecuadas a adoptar, a partir de una alteración que afecte al cálculo del riesgo y de modo que el impacto causado sea mínimo. En el ejemplo expuesto en [34] ante una nueva vulnerabilidad el árbol recorre las posibles acciones alternativas que permitirían paliarla, asumiendo el menor riesgo posible, como se recoge en la Fig. 5. La generación de estos árboles requiere un proceso de aprendizaje supervisado (Reinforcement Learning), basado en aplicación de Redes Neuronales conforme detalla [35].

2) ***Automatización de la respuesta frente a incidentes****:* La detección de incidentes por parte de sistemas IDS/IPS debe ser complementada idealmente, por una respuesta lo más efectiva y rápida posible. La automatización de esta respuesta, mediante los Automated Intrusion Response System (AIRS) como recoge [15] provee cuanto menos la eficacia perseguida si bien debe garantizarse que su efectividad se maximiza, frente a la respuesta humana de un analista o administrador, capacitado para poner en contexto dicha alarma y actuar de la manera más adecuada. En [36] se presenta el método Rheo-Stat, enfocado a la respuesta automática ante alertas del IDS basadas en restringir los permisos de ejecución en el sistema, a los procesos asociados al intento de intrusión, en base al riesgo percibido. Estas respuestas automatizadas tienen uno de sus puntos débiles, en el tratamiento de los falsos positivos. La aplicación de medidas en este tipo de situaciones, que no responden a un incidente real, puede resultar en un derroche de recursos de seguridad que incluso afecten al desarrollo normal de la actividad. Esfuerzos como [36] se centran en soslayar este problema mediante un modelo de fusión en diferentes fases, que consiste en analizar la información suministrada por los IDS a tres niveles: un primero de composición de las diferentes alertas de los IDS, para obtener el incidente raíz que las genera; un segundo de identificación de la amenaza y asignación de su severidad y prioridad; y un tercero de valoración y distribución del riesgo en el conjunto de la red.

IV. Conclusiones y Trabajo Futuro

Si bien en muchos casos de los estudiados y mencionados anteriormente se tratan dinámicas y evolución en el tiempo de los riesgos, como es fundamentalmente el caso de los árboles y grafos de ataque o de decisión, éstos se han enfocado fundamentalmente al análisis estático de los diferentes escenarios preconcebidos, si bien, se prestan al seguimiento en tiempo real de la evolución de un riesgo e incluso la aplicación automatizada de medidas para su gestión. A nivel técnico, las herramientas que actualmente ofrecen la monitorización de amenazas o vulnerabilidades en tiempo real (i.e.: SIEM, IDS e IPS) aportan una visión del riesgo poco generalista y no alineada con las metodologías de riesgo que se emplean para la visión a nivel directivo. Esta falta de consenso entre el riesgo percibido a bajo y a alto nivel podría repercutir en la toma de decisiones no alineadas con los objetivos de negocio, políticas de seguridad, etc. La posibilidad de integrar en un cuadro de mandos el ciclo dinámico de AARR ofrecería una capacidad adicional de toma de decisiones a alto nivel para enfrentar o monitorizar situaciones de crisis en tiempo real. La necesidad

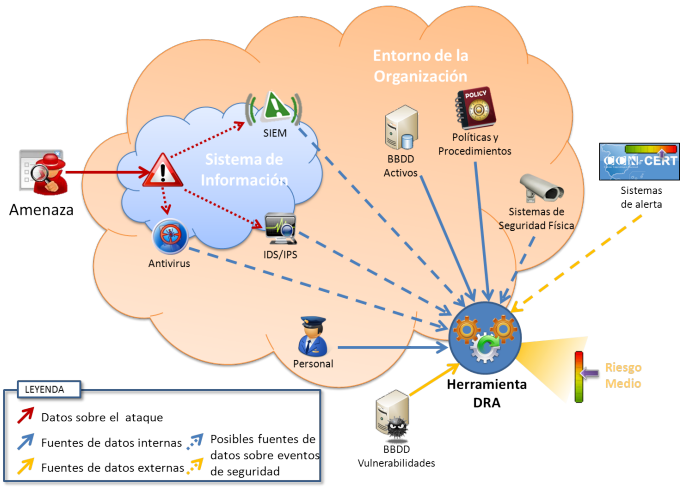

Fig. 3. Evaluación Dinámica del Riesgo integrando sistemas de seguridad

de obtener información continua que realimente la evaluación del riesgo, implica el desarrollo de interfaces o estándares que permitan establecer una adecuada comunicación entre los múltiples tipos de sistemas que rodean el ámbito de la seguridad (ya sea física o de la información) de forma que los datos estandarizados puedan ser utilizados por herramientas que implementen las metodologías de AARR (DRA). Estos datos deberían ser adecuadamente filtrados por las herramientas de seguridad antes de su envío para que la herramienta DRA no se vea saturada de información irrelevante. Del mismo modo, el

cálculo probabilístico del riesgo que debería basarse en fuentes objetivas y lo más profusas posible, se vería enriquecido por un intercambio y una cooperación a nivel de conocimiento sobre incidentes, amenazas y vulnerabilidades.

El planteamiento de trabajo futuro se orienta a la evolución de este concepto de comunicaciones adaptadas a diferentes naturalezas de fuentes de información (ver Fig. 3), sobre eventos de seguridad u otros aspectos relevantes cuyos datos sean de utilidad para el cálculo del AARR Dinámico y finalmente la Gestión Dinámica del Riesgo.

AGRADECIMIENTOS

Los autores agradecen la financiación que les brinda el Subprograma AVANZA COMPETITIVIDAD I+D+I del Ministerio de Industria, Turismo y Comercio (MITyC) a través del Proyecto TSI-020100-2011-165. Asimismo, los autores agradecen la financiación que les brinda el Programa de Cooperación Interuniversitaria de la Agencia Española de Cooperación Internacional para el Desarrollo (AECID), Programa PCI-AECID, a través de la Acción Integrada MAEC-AECID MEDITERRÁNEO A1/037528/11.

REFERENCIAS

[1] ISO 31000:2009, *Risk management - Principles and guidelines*, International Organization for Standardization, ISOIEC, 2009.

[2] ISO 27005:2008, *Information technology - Security techniques - Information security risk management*, ISOIEC, 2008.

[3] UNE 71504:2008, *Tecnología de la Información (TI) - Metodología de análisis y gestión de riesgos para los sistemas de información*, AENOR, 2008.

[4] MAGERIT versión 2, *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. I Método*, Ministerio de Administraciones Públicas (MAP), España, 2006.

[5] C. Alberts, and A. Dorofee "Managing Information Security Risk. The OCTAVE Approach", in Addison Wesley, 2005.

[6] Siemens - Insight Consulting, *The Logic behind CRAMM's Assessment of Measures of Risk and Determination of Appropriate Countermeasures*, Siemens, 2005.

[7] EBIOS v2: *Méthode pour l'Expression des Besoins et l'Identification des Objectifs de Sécurité*, Direction Centrale de la Sécurité des Systèmes d'Information (DCSSI), France, 2004.

[8] BSI *IT Baseline Protection Manual Bundesamt für Sicherheit in der Informationstechnik* Federal Office for Information Security (BSI), Deutschland, 2000.

[9] G. Stoneburner, A. Goguen, and A. Feringa, "Risk Management Guide for Information Technology Systems", in *NIST Special Publication 800-30*, 2002.

[10] Technical Department of ENISA, Section Risk Management, *Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools*, European Network and Information Security Agency (ENISA), 2006.

[11] ISO 27001:2005, *Information technology - Security techniques - Information security management systems - Requirements*, ISOIEC, 2005.

[12] NIST, "Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach", en *NIST Special Publication 800-37*, rev. 1, 2010.

[13] W. Qi, X. Liu, J. Zhang, and W. Yuan, "Dynamic Assessment and VaR-Based Quantification of Information Security Risk", in *2nd International e-Business and Information System Security Conference (EBISS)*, pp.1-4, 22-23, 2010.

[14] P. Lagadec, "Visualization et Analyse de Risque Dynamique pour la Cyber-Défense", in *Symposium sur la sécurité des technologies de l'information et des communications (SSTIC)*, 2010.

[15] C.P. Mu, X.J. Li, H.K. Huang, and S.F. Tian, "Online Risk Assessment of Intrusion Scenarios Using D-S Evidence Theory", in *European Symposium on Research in Computer Security (ESORICS)*, pp.35-48, 2008.

[16] H. Kjetil, A. Ajith, and J.K. Svein, "DIPS: A Framework for Distributed Intrusion Prediction and Prevention Using Hidden Markov Models and Online Fuzzy Risk Assessment", in *Third International Information Assurance and Security Symposium (IAS)*, pp.183-190, 2007.

[17] H. Zhi-Hua, D. Yong-Sheng, and H. Jing-Wen, "Knowledge Based Framework for Real-Time Risk Assessment of Information Security Inspired by Danger Model", in *International Conference on Security Technology (SECTECH '08)*, pp.91-94, 13-15, Dec. 2008.

[18] W.D. Jones, S.J. Aud, J.P. Hudepohl, M.L. Flournory, W.B. Snipes, and E.C. Schutz, "Method and System for Dynamic Risk Assessment of Software", in *United States Patents*, Patent no: US 6219805 B1, 2001.

[19] National Institute of Standards and Technology (NIST) "National Vulnerability Database", [Online]. Available: http://nvd.nist.gov

[20] P.A.S. Ralstona, J.H. Grahamb, and J.L. Hiebb, "Cyber security risk assessment for SCADA and DCS networks", in *ISA Transactions*, vol. 46, pp.583, 2007.

[21] J.A. Mañas, and C. Belso, "Gestión Dinámica de Riesgos: Seguridad de la Red de Servicios", in *XI jornadas sobre tecnologías de la información para la modernización de las administraciones públicas*, 2010.

[22] N. Poolsappasit, R. Dewri, and I. Ray, "Dynamic Security Risk Management Using Bayesian Attack Graphs", in *IEEE Transactions on Dependable and Secure Computing*, vol.9, no.1, pp.61-74, Jan.-Feb. 2012.

[23] Y.Y. Haimes, J.R. Santos, K.G. Crowther, M. Henry, C. Lian, and Z. Yan, "Risk Analysis in Interdependent Infrastructures", in *Critical Infrastructure Protection'2007*, pp.297-310, 2007.

[24] Y.Y. Haimes, J.R. Santos, and K.G. Crowther, "Analysis of Interdependencies and Risk in Oil & Gas Infrastructure Systems", in *Center for Risk Management of Engineering Systems University of Virginia*, Research Report, no.11, Jun. 2007.

[25] R. Dantu, K. Loper, and P. Kolan, "Risk management using behavior based attack graphs", in *Proceedings of International Conference on Information Technology: Coding and Computing (ITCC'2004)*, vol.1, pp.445-449 Vol.1, 5-7, Apr. 2004.

[26] R. Dantu, P. Kolan, R. Akl, and K. Loper, "Classification of Attributes and Behavior in Risk Management Using Bayesian Networks", in *Intelligence and Security Informatics, 2007 IEEE*, pp.71-74, May. 2007.

[27] M. Henry, and Y. Haimes, "A comprehensive network security risk model for process control networks", in *Risk Analysis*, vol.29, no.2, pp.223-248, 2009.

[28] M. Nicolett, and K.M. Kavanagh, "Magic Quadrant for Security Information and Event Management (SIEM)", in *Gartner*, Research Report, no.G00176034, May. 2010.

[29] A. Arnes, K. Sallhammar, K. Haslum, T. Brekne, M.E. Gaup Moe, and S.J. Knapskog, "Real-time Risk Assessment with Network Sensors and Intrusion Detection Systems", in *International Conference on Computational Intelligence and Security (CIS-05)*, Xian, China, published in Springer LNCS vol.3801/3802, Dec. 2005.

[30] M. Swimmer, "Using the danger model of immune systems for distributed defense in modern data networks", in *Computer Networks*, no.51, pp.1315-1333, 2007.

[31] K. Voss, Ch. Carlsson, and A. Akademi, "Consultant Service and Dynamic Risk Assessment", in *IST-AssessGrid project WP.3*, Sixth Framework Programme, 2008.

[32] C. Fu, J. Ye, L. Zhang, Y. Zhang, and H. LanSheng, "A Dynamic Risk Assessment Framework Using Principle Component Analysis with Projection Pursuit in Ad Hoc Networks", in *Ubiquitous Intelligence & Computing, and 7th International Conference on Autonomic & Trusted Computing (UIC/ATC)*, pp.154-159, 26-29, Oct. 2010.

[33] N. Ming, J.D. McCalley, V. Vittal, and T. Tayyib, "Online risk-based security assessment", in *IEEE Transactions on Power Systems*, vol.18, no.1, pp. 258-265, Feb. 2003.

[34] L. Beaudoin, N. Japkowicz, and S. Matwin, "Autonomic Computer Network Defence Using Risk State and Reinforcement Learning", in *Cryptology and Information Security Series*, vol.3, pp.238-248, 2009.

[35] L. Beaudoin, N. Japkowizc, and S. Matwin, "Autonomic Computer Network Defence Using Risk States and Reinforcement Learning", Thesis manuscript, University of Ottawa, 2009.

[36] A. Gehani, and G. Kedem, "RheoStat: Real-time Risk Management", in *Proceedings of the 7th International Symposium on Recent Advances in Intrusion Detection*, pp.15-17, 2004.

[37] J. Ma, Z. Li, and H. Zhang, "A Fusion Model for Network Threat Identification and Risk Assessment", in *International Conference on Artificial Intelligence and Computational Intelligence, (AICI'09)*, vol.1, pp.314-318, 7-8, Nov. 2009.