



PROYECTO FIN DE  
MÁSTER EN SISTEMAS INTELIGENTES  
CURSO 2011-2012

---

**ANÁLISIS DE RIESGOS DINÁMICOS EN  
SISTEMAS DE INFORMACIÓN**

**David López Cuenca**

Director:

**Luis Javier García Villalba**

Departamento de Ingeniería del Software e Inteligencia Artificial

---

MÁSTER EN INVESTIGACIÓN EN INFORMÁTICA  
FACULTAD DE INFORMÁTICA  
UNIVERSIDAD COMPLUTENSE DE MADRID

*CONVOCATORIA: JUNIO/2012*

*CALIFICACIÓN: SOBRESALIENTE (9)*



## **AUTORIZACIÓN DE DIFUSIÓN**

DAVID LÓPEZ CUENCA

11/07/2012

El/la abajo firmante, matriculado/a en el Máster en Investigación en Informática de la Facultad de Informática, autoriza a la Universidad Complutense de Madrid (UCM) a difundir y utilizar con fines académicos, no comerciales y mencionando expresamente a su autor el presente Trabajo Fin de Máster: “ANÁLISIS DE RIESGOS DINÁMICOS EN SISTEMAS DE INFORMACIÓN”, realizado durante el curso académico 2011-2012 bajo la dirección de Luis Javier García Villalba en el Departamento de Ingeniería del Software e Inteligencia Artificial, y a la Biblioteca de la UCM a depositarlo en el Archivo Institucional E-Prints Complutense con el objeto de incrementar la difusión, uso e impacto del trabajo en Internet y garantizar su preservación y acceso a largo plazo.



## **RESUMEN EN CASTELLANO**

Actualmente, 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 propone una extensión al modelo de datos IODEF orientada al Análisis de Riesgos Dinámico (IODEF-DRA). Este modelo tiene por objetivo facilitar una visión global del riesgo, a través de la integración en tiempo real y mediante comunicaciones basadas en él, de un amplio abanico de sistemas de seguridad con herramientas de Análisis de Riesgos (basadas en metodologías reconocidas). La utilidad de esta integración se refleja en el escenario presentado como prueba de concepto, donde se evidencian las posibles mejoras en los resultados del Análisis de Riesgos.

## **PALABRAS CLAVE**

Análisis de Riesgos Dinámico, Dynamic Risk Assessment, Online Risk Assessment, Real Time Risk Assessment, IODEF-DRA.



## **RESUMEN EN INGLÉS**

Nowadays Risk Management is a common practice in the Information Systems security field. It is usually supported by a Risk Assessment process done at regular intervals, instead of dynamically.

In this paper different existing approaches to face Dynamic Risk Assessment and Management are recapitulated along with their pros and cons. As a result of this analysis, the IODEF extended model for Dynamic Risk Assessment (IODEF-DRA) is presented.

This data model aims to facilitate a global vision of risk, by letting RA tools based on renowned methodologies, be fed in real-time with security events data from a wide range of security systems. Usefulness of this integration and the proposed data model is presented through a proof-of-concept scenario, where improvements on risk assessment outcomes are evidenced.

## **KEYWORDS**

Dynamic Risk Assessment, Online Risk Assessment, Real Time Risk Assessment, IODEF-DRA.





## **AGRADECIMIENTOS**

Mi agradecimiento más sincero a quienes, a lo largo de mi experiencia profesional me han involucrado, y transmitido sus conocimientos, en el área de la seguridad de la información permitiéndome vislumbrar su magnitud y los desafíos que implica.

Del mismo modo, gracias a la confianza depositada por Javier García Villalba y a su apoyo a lo largo del último año, que han dado como resultado este proyecto, así como los congresos y publicaciones que han salido adelante.

Por supuesto, gracias a mi familia y amigos que a lo largo de mi vida me han llevado a ser quien soy, y a estar donde estoy.

Y finalmente, **GRACIAS a Estrella...** por ser ella y por estar ahora y siempre ahí, iluminando el camino.



## LISTADO DE ACRÓNIMOS

<b>AARR</b>	Análisis de Riesgos
<b>ADN</b>	Autonomic Defense Network
<b>AIRS</b>	Automated Intrusion Response System
<b>BBDD</b>	Bases de Datos
<b>CERT</b>	Computer Emergency Response Team
<b>CMMI</b>	Capability Maturity Model Integration
<b>CSIRT</b>	Computer Security Incident Response Teams
<b>DAG</b>	Directed Acyclic Graph
<b>DRA</b>	Dynamic Risk Assessment
<b>ENISA</b>	European Network and Information Security Agency
<b>EMS</b>	Energy Management Systems
<b>FTP</b>	File Transfer Protocol
<b>HIDS</b>	Host-based Intrusion Detection System
<b>HMM</b>	Hidden Markov Models
<b>HCBM</b>	Hierarchical Coordinated Bayesian Model
<b>IDMEF</b>	Intrusion Detection Message Exchange Format
<b>IDS</b>	Intrusion Detection System
<b>IETF</b>	Internet Engineering Task Force
<b>INCH</b>	Incident Handling
<b>IODEF</b>	Incident Object Description and Exchange Format
<b>IPS</b>	Intrusion Prevention System
<b>ISAC</b>	Information Sharing and Analysis Center
<b>ISO</b>	International Organization for Standardization
<b>NIDS</b>	Network Intrusion Detection System
<b>OCDE</b>	Organización de Cooperación y Desarrollo Económico
<b>OTAN</b>	Organización del Tratado del Atlántico Norte
<b>RFC</b>	Request For Comments
<b>ROI</b>	Return On Investment
<b>SCADA</b>	Supervisory Control And Data Acquisition

<b>SGSI</b>	Sistema de Gestión de la Seguridad en la Información
<b>SIEM</b>	Security Information and Event Management
<b>SLA</b>	Service Level Agreement
<b>SSII</b>	Sistemas de la Información
<b>TIC</b>	Tecnologías de la Información y las Comunicaciones
<b>WG</b>	Working Group
<b>XML</b>	Extensible Markup Language

# ÍNDICE DE CONTENIDOS

<b>1</b>	<b>OBJETIVOS Y ESTRUCTURA DEL PROYECTO .....</b>	<b>1</b>
<b>2</b>	<b>INTRODUCCIÓN AL ANÁLISIS Y A LA GESTIÓN DEL RIESGO .....</b>	<b>2</b>
2.1	El Análisis y la Gestión del Riesgo.....	4
2.2	Metodologías de Análisis y Gestión del Riesgo .....	7
2.3	Conceptos y Terminología Básicos .....	9
<b>3</b>	<b>ANÁLISIS Y GESTIÓN DINÁMICA DEL RIESGO .....</b>	<b>14</b>
3.1	Concepto .....	15
3.2	Objetivos .....	19
3.3	Evolución del Análisis de Riesgos Dinámico.....	19
3.3.1	Alimentación desde BBDD.....	20
3.3.2	Grafos y Árboles de ataque.....	20
3.3.3	Enfoque mixto.....	23
3.3.4	Monitorización de estado del sistema .....	24
3.4	Evolución del Tratamiento Dinámico del Riesgo.....	26
3.4.1	Árboles de decisión para optimización del riesgo .....	26
3.4.2	Automatización de la respuesta frente a incidentes .....	27
3.5	Áreas de Mejora Observadas .....	28
<b>4</b>	<b>COMUNICACIÓN DE EVENTOS DE SEGURIDAD PARA ANÁLISIS DE RIESGOS DINÁMICO.....</b>	<b>30</b>
4.1	Motivación de la Propuesta de Trabajo .....	31
4.2	Modelos de Datos Relacionados con la Gestión de Incidentes.....	34
4.2.1	Intrusion Detection Message Exchange Format (IDMEF) .....	34
4.2.2	Incident Object Description and Exchange Format (IODEF).....	37
4.3	Extensión de un Modelo de Datos para Comunicación de Eventos de Seguridad Enfocados al Análisis de Riesgos Dinámico .....	42
4.4	Prueba de Concepto de Análisis de Riesgos Dinámico mediante el Modelo IODEF-DRA	51
<b>5</b>	<b>CONCLUSIONES Y TRABAJO FUTURO.....</b>	<b>56</b>
5.1	Trabajo Futuro .....	57
5.2	Divulgación de Resultados .....	58

<b>REFERENCIAS .....</b>	<b>59</b>
<b>APÉNDICE A - EJEMPLO DE MENSAJES IODEF-DRA PARA PRUEBA DE CONCEPTO (XML)...</b>	<b>64</b>

## ÍNDICE DE FIGURAS

Figura 2.1 - Evolución en el tiempo del Análisis de Riesgos .....	3
Figura 2.2 - Proceso de Gestión del Riesgo para la Seguridad de la Información .....	5
Figura 2.3 - Diagrama de conceptos genéricos implicados en el Análisis de Riesgos .....	9
Figura 2.4 - Resumen de conceptos genéricos implicados en el Análisis de Riesgos .....	12
Figura 3.1 - Modelo PDCA aplicado al Sistema de Gestión de Seguridad en la Información.....	15
Figura 3.2 - Principales variables involucradas en Análisis de Riesgos de Sist. Información .....	16
Figura 3.3 - Flujo de un DRA basado en un bucle reiterativo, en base a un AARR estático .....	18
Figura 3.4 - Representación de un grafo de ataque.....	22
Figura 3.5 - Árbol de optimización de tratamiento de vulnerabilidades por riesgo .....	27
Figura 4.1 - Evaluación del Riesgo NO integrada .....	31
Figura 4.2 - Evaluación del Riesgo Integrada.....	33
Figura 4.3 - Modelo de Datos IDMEF.....	36
Figura 4.4 - Modelo de Datos IODEF (versión inicial del IODEF WG).....	39
Figura 4.5 - Modelo de Datos IODEF (versión final del IODEF INCH) .....	41
Figura 4.6 - Modelo de Datos IODEF extendido para AARR Dinámico (IODEF-DRA).....	47
Figura 4.7 - Ejemplo de árbol de ataque para la prueba de concepto de IODEF-DRA.....	51
Figura 4.8 - Evolución del riesgo calculado en el árbol de ataque mediante DRA .....	54





# 1 OBJETIVOS Y ESTRUCTURA DEL PROYECTO

---

La observación acumulada en base a la experiencia como auditor y consultor de seguridad, en torno a la utilidad y limitaciones de la aplicación de los Análisis de Riesgos y los procesos de Gestión del Riesgo en los Sistemas de Información, llevan a atisbar un amplio margen de desarrollo y mejora de los mecanismos utilizados.

El presente proyecto pretende acotar aquellos ámbitos que ofrecen mayores oportunidades en este sentido, fijando la vista en un terreno aún poco explotado, como es el de añadir una componente dinámica al proceso de Análisis y Gestión del Riesgo.

Así, el Capítulo 2 se centra en introducir el concepto de Gestión del Riesgo, con especial interés en una de sus fases como es la del Análisis del Riesgo, poniendo sobre la mesa los estándares, prácticas y metodologías más aceptadas y que servirán como fundamento o pilar para el resto del estudio.

La evolución que estos conceptos han seguido en el tiempo hacia un modelo dinámico, basada en un detallado análisis de la literatura existente en este ámbito, se refleja a lo largo del Capítulo 3 mostrando el estado del arte en torno al Análisis y Gestión Dinámica del Riesgo. En él se apunta ya, hacia las posibles áreas de mejora en dicho campo, una de las cuáles se materializará en un desarrollo posterior, como aportación original de este proyecto.

El Capítulo 4 recoge una de las áreas de mejora denotadas en el capítulo anterior, para materializar una visión global y metodológica así como en tiempo real del riesgo, a través de un modelo de datos IODEF-DRA que permita la comunicación de eventos de seguridad entre sistemas de seguridad de diferente naturaleza y herramientas de Análisis de Riesgos Dinámicos. Para ello, se analizan modelos de datos ya existentes, adaptando el que se estima más apropiado (IODEF) para el uso pretendido. En el mismo capítulo se presenta una prueba de concepto que ilustra el uso del modelo en un escenario predefinido, recogándose en el Apéndice A el detalle de las comunicaciones que se generarían en base al nuevo modelo propuesto (IODEF-DRA).

## **2 INTRODUCCIÓN AL ANÁLISIS Y A LA GESTIÓN DEL RIESGO**

---

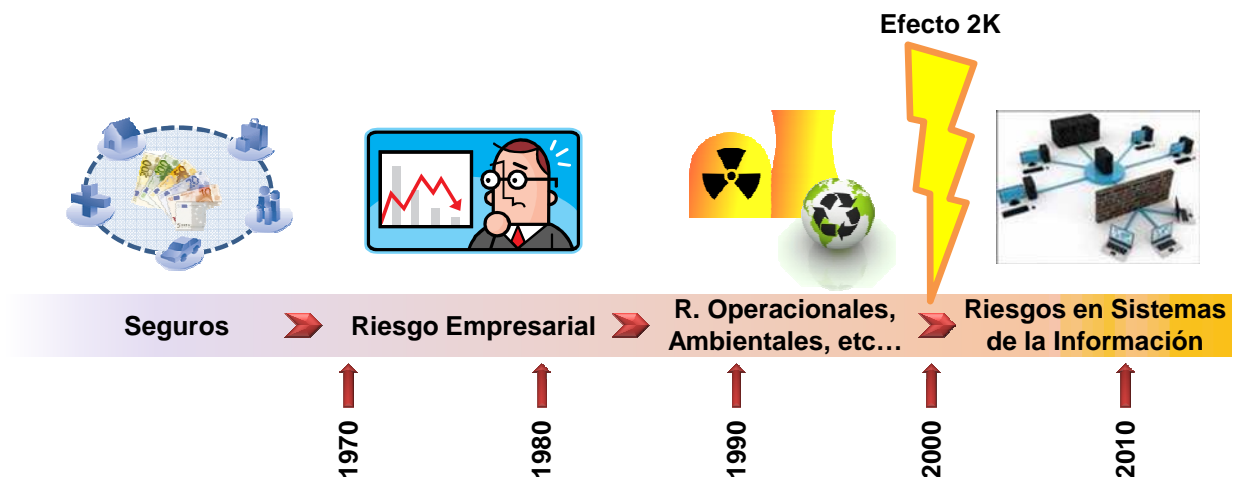
La Gestión del Riesgo nace de la necesidad de organizar e interpretar datos científicos y otras informaciones, facilitando la toma de decisiones y los acuerdos. El interés por poder determinar con anticipación los eventos del futuro, supuso el pilar de un área de la matemática aplicada conocida inicialmente como Teoría de Juegos (John von Neumann – 1926).

Durante la primera mitad del Siglo XX, el campo que monopoliza el análisis de los riesgos es el del negocio de los seguros, en torno a los que existe una profusa bibliografía. Es en este terreno en el que se comienza a forjar la relación coste-riesgo.

La Gestión del Riesgo, como disciplina, emerge a mediados de la década de los 70, como una evolución del campo de la Gestión de Seguros, terreno en el que se comienza a forjar la relación coste-riesgo, adaptando su nomenclatura al hecho de que su enfoque pasa a ser mucho más amplio. En las décadas de los 80 y 90 la Gestión del Riesgo se integró efectivamente en las compañías convirtiéndose en una parte vital de su planificación y estrategias. Conforme el papel que juega, abarca una mayor escala, este campo comienza a conocerse como Gestión del Riesgo Empresarial. A lo largo de los 90, emergen nuevas áreas en relación a la Gestión del Riesgo. Conforme a la “Risk and Insurance Management Society (RIMS)”, destacan las relativas a Gestión de Operaciones, Riesgos Ambientales y Riesgos Éticos.

En torno a finales del siglo XX se comienza a conceder mayor relevancia a los efectos sobre el negocio, de los riesgos introducidos por las nuevas tecnologías, siendo el efecto 2000 un hito a este respecto. En los años previos (1995) se publicaban los primeros estándares de Seguridad de la Información (BS 7799-1) adoptado precisamente en el año 2000 como el estándar ISO/IEC 17799, contemplando ya la gestión del riesgo como parte del proceso de seguridad. El efecto mediático de eventos como los atentados del World Trade Center o fraudes corporativos de magnitud, llevan a incentivar el desarrollo de este campo desde las administraciones, para evitar y/o afrontar situaciones similares.

Esta evolución del análisis y la gestión de riesgos, a través de los diferentes ámbitos que la han abrazado, se recoge de modo simplificado en la línea de tiempo añadida como *Figura 2.1*.



**Figura 2.1 - Evolución en el tiempo del Análisis de Riesgos**

Actualmente existen requisitos normativos en torno a la protección de infraestructuras tecnológicas y de la información, que exigen la realización de Análisis de Riesgos como parte de los esfuerzos por protegerlos adecuadamente, en beneficio del interés común e individual. Los principales cuerpos legislativos que materializan esta necesidad son los referidos a la protección de Infraestructuras Críticas [1,2], el Esquema Nacional de Seguridad [3], el Acceso Electrónico de los Ciudadanos a los Servicios Públicos [4] y las Políticas de Seguridad TIC para la Administración [5], a lo que se suman estándares y buenas prácticas como las Directrices de la OCDE (Organización de Cooperación y Desarrollo Económico) para la Seguridad de Sistemas y Redes de Información, el estándar ISO 27005:2008 que da las pautas en relación a los Análisis de Riesgos en Sistemas de Gestión de la Seguridad en la Información (SGSI), etc.

## 2.1 El Análisis y la Gestión del Riesgo

La Gestión del Riesgo<sup>1</sup> 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.

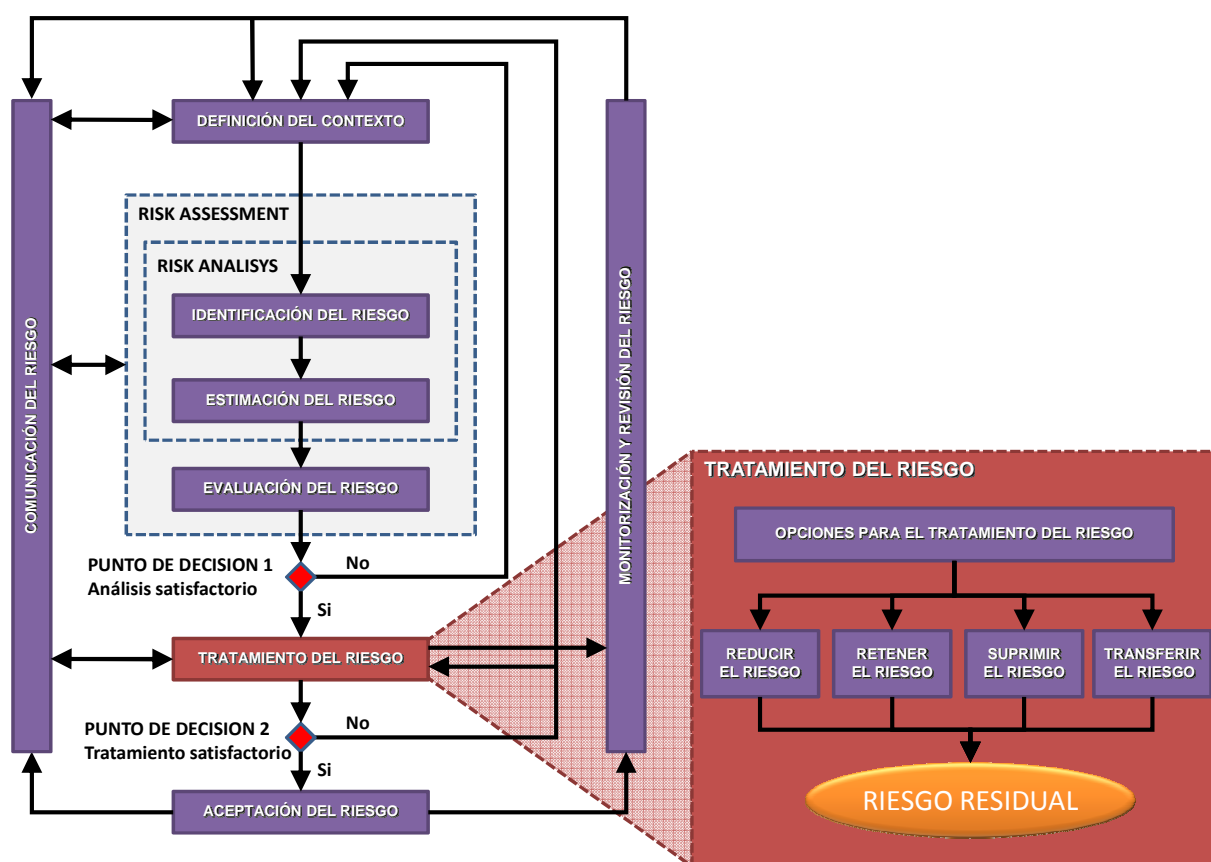
Con este fin, la Gestión del Riesgo se apoya en el Análisis de Riesgos (en adelante AARR). El AARR es, conforme a [6], el proceso que permite identificar, estudiar y evaluar a través de las diferentes variables implicadas, los potenciales eventos que afecten a, y sus consecuencias para, los objetivos de una organización. Para ello, realiza una predicción del futuro, basándose en el pasado histórico y un análisis cuidadoso de los eventos. El AARR no reemplaza la experiencia empírica, por el contrario, con frecuencia gran cantidad de información se obtiene a partir de juicios de expertos. Los juicios, toman la forma de una distribución de probabilidades y siguen todas las reglas de la teoría tradicional de probabilidades.

Una vez conocidos los riesgos, éstos pueden ser tratados de diferentes maneras, que en la mayoría de los casos requieren una cierta inversión en medios y medidas de seguridad, o soluciones alternativas con mayor o menor coste asociado. La Gestión del Riesgo pretende facilitar la labor de toma de decisiones en torno a los riesgos que requieren un tratamiento y de la mejor alternativa para dicho tratamiento. Es fundamental optimizar la relación coste-beneficio, de modo que la inversión en seguridad no sea superior a la pérdida que el riesgo podría provocar en caso de materializarse, asumiéndose que es inevitable la necesidad de aceptar un nivel de riesgo, que debe ser conocido y limitado a un valor umbral.

---

<sup>1</sup> La Red Temática CRIPTORED ofrece una introducción muy ilustrativa al Análisis y Gestión de los Riesgos a través del proyecto Intypedia: <http://www.criptored.upm.es/intypedia/video.php?id=introduccion-gestion-riesgos&lang=es>

Puesto que el riesgo es un concepto dinámico que varía con el transcurso del tiempo y con las modificaciones en los múltiples factores que definen dicho riesgo, la Gestión del Riesgo establece el seguimiento y el análisis continuo de su evolución. Esta reiterada aplicación de AARR de cara a monitorizar los cambios surgidos, requiere que los análisis puedan ser contrastados manteniendo la necesaria coherencia para poder obtener resultados válidos de tal comparación.



**Figura 2.2 - Proceso de Gestión del Riesgo para la Seguridad de la Información<sup>2</sup>**

Los estándares ISO a través de su serie 27000 establecen que, para una adecuada implantación de un SGSI, debe realizarse una Gestión del Riesgo basada en un AARR. El proceso conforme se recoge en la *Figura 2.2*, cuenta con una fase de identificación-estimación-evaluación del riesgo (en torno al contexto previamente definido), seguida de una de tratamiento

<sup>2</sup> Adaptación del original publicado en [7]

del riesgo en base a los resultados de la fase anterior. La situación en relación al riesgo debe ser adecuadamente comunicada a los afectados dentro de la Organización de modo que exista una apropiada concienciación, mientras que en paralelo se supervisa y revisa la evolución del riesgo en el tiempo, reiterando periódicamente el proceso.

La fase de tratamiento del riesgo toma como entrada los riesgos evaluados previamente, correspondiendo a los responsables de la Organización decidir cuál de las siguientes opciones se aplican:

- ***Reducción del Riesgo:*** Mediante la aplicación de controles que los mitiguen o eliminen.
- ***Retención del Riesgo:*** La aplicación de medidas puede no resultar efectiva o no considerarse justificada en algunos casos. Los riesgos que no superen un determinado umbral en base a los criterios establecidos por la Organización, o no tratados mediante alguna de las otras opciones, se consideran retenidos.
- ***Supresión del Riesgo:*** Supone la eliminación del proceso o condición que origina el riesgo, si bien en múltiples ocasiones no es factible, ya que éstos resultan elementos imprescindibles para la Organización.
- ***Transferencia del Riesgo:*** La transferencia de riesgos permite traspasar la responsabilidad en su tratamiento a terceros con capacidad para ello, siendo un ejemplo fundamental la contratación de seguros.

Las opciones seleccionadas pueden aplicarse mediante un Plan de Tratamiento del Riesgo que las acometa en plazos diferenciados conforme a su prioridad. El riesgo remanente tras el proceso de tratamiento es conocido como Riesgo Residual y debe ser formalmente aceptado, asumiéndose por parte de la Organización.

## 2.2 Metodologías de Análisis y Gestión del Riesgo

El proceso de AARR comprende un ejercicio de comprensión, catalogación y valoración de aspectos que adquieren gradualmente una complejidad sustancial. A ello se suma el hecho de que estos aspectos llevan asociados inevitablemente un grado elevado de subjetividad, en particular cuando se soportan en el juicio de expertos, en lugar de basarse en datos o registros cuantitativos.

Sin embargo, un AARR de utilidad para la Gestión del Riesgo debe ser riguroso y permitir ser contrastado y comparado de manera objetiva. De otro modo se podría inducir un sesgo, que condicione las decisiones basadas en los resultados del AARR afectando a su fiabilidad y efectividad.

Es por ello que se persigue una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista. Una metodología ofrece a nivel teórico las siguientes ventajas:

- Evita la improvisación, así como una aproximación excesivamente técnica.
- Permite conseguir una aproximación global y completa.
- Permite aprovechar lo ya hecho y dar continuidad al esfuerzo invertido.
- Aporta rapidez, uniformidad, consistencia y rigor.
- Garantiza que se tengan en consideración todos los factores.
- Facilita la “Auditabilidad” (queda constancia de lo hecho).
- Aumenta la objetividad en los criterios.
- Establece una sistemática.
- No hay dependencia total de quién lo ha hecho.

Existen múltiples metodologías para el AARR en función del campo de aplicación, entre las que figuran: MOSLER (seguridad física), GRETENER (riesgo de incendio), SCORE (riesgos sanitarios), etc.

En el campo de las Tecnologías de la Información, destacan las normas y metodologías de Análisis y Gestión del Riesgo mostradas a continuación, fundamentalmente patrocinadas por los organismos que se mencionan respectivamente:

- **ISO 27005:2008** (IEC - Internacional) [7].
- **UNE 71504:2008** (AENOR - España) [8].
- **MAGERIT** (Ministerio de Administraciones Públicas - España) [9].
- **OCTAVE** (SEI Carnegie Mellon University - USA) [10].
- **CRAMM** (Siemens Insight Consulting - UK) [11].
- **EBIOS** (DCSSI - Francia) [12].
- **IT Baseline Protection Manual** (BSI - Alemania) [13].
- **NIST SP800-30** (NIST - USA) [14].
- Otras: **MÉHARI**, **COBRA**, **ISAAC**, **RA2**, etc.

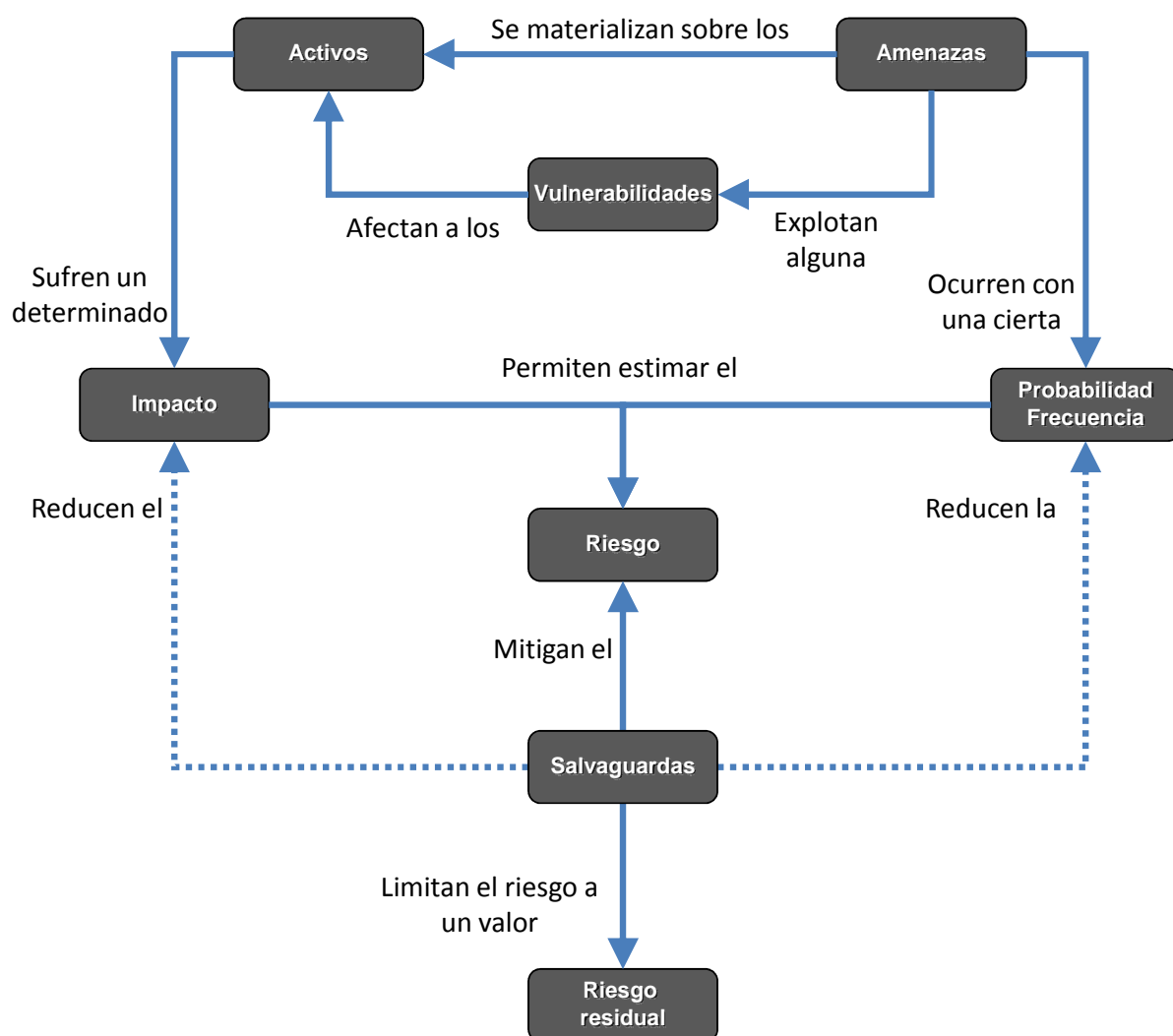
Existen herramientas que simplifican la aplicación de algunas de estas metodologías, aportando una base de conocimiento, flujos de trabajo, automatización de cálculos, e interfaces que mejoran el desarrollo del análisis y el procesamiento de los resultados.

La European Network and Information Security Agency (ENISA) publica un catálogo [15] 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. Adicionalmente, el catálogo facilita la comparativa entre las diferentes metodologías y herramientas.



## 2.3 Conceptos y Terminología Básicos

En general, las metodologías mencionadas anteriormente parten de conceptos similares, con algunos matices. Dichos conceptos son los que se recogen de manera genérica en [7], quedando plasmados en la *Figura 2.3*.



**Figura 2.3 - Diagrama de conceptos genéricos<sup>3</sup> implicados en el Análisis de Riesgos**

<sup>3</sup> 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>

La definición de cada uno de los conceptos se recopila a continuación, resumiéndose posteriormente en la *Figura 2.4*:

#### ***a) Activos***

Cuando hablamos de activos de los SSII, se puede englobar no sólo el Hardware, Redes y Software (que serían los más evidentes), sino también todos aquellos que los soportan, utilizan o afectan en alguna medida, como por ejemplo: el personal (administradores, usuarios, etc.), infraestructuras (edificios o suministros) u otros más intangibles como la propia información, la imagen o la reputación.

En cualquier caso, los activos son relevantes en función del valor que tengan para la Organización. Habitualmente, los activos mantienen relaciones unos con otros, creándose una jerarquía de dependencias. Estas dependencias influyen, determinando el valor de un activo, en función de los activos a los que asiste.

Existen dos métodos para estimar el valor de un activo:

- *Cuantitativo*: en el que se asigna un valor económico en función de su precio, coste de reposición u otros factores que influyan en ello.
- *Cualitativo*: En el que el valor oscila dentro de una escala limitada y progresiva, utilizando valores como “Bajo”, “Medio” o “Alto”, o cifras en un conjunto entre dos límites definidos.

#### ***b) Amenazas***

Las 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. Las amenazas podrían ser de diferente naturaleza: acción humana voluntaria o involuntaria, elemento natural o ambiental, etc.

#### ***c) Vulnerabilidades***

Defecto o debilidad en los procedimientos, diseños, implementaciones o controles internos de seguridad de los sistemas que pueden ser explotados (accidental o intencionadamente), provocando una brecha de seguridad o una violación de la política de seguridad de los sistemas.

***d) Impacto***

Es el 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 su valor.

***e) Frecuencia / Probabilidad***

La probabilidad es un indicador de posibilidad, que determina si una potencial vulnerabilidad puede acontecer 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.

Estos indicadores pueden resultar más fácilmente estimables en ataques no deliberados (naturales, industriales) o basados en series históricas (análisis estadístico). Por el contrario resulta difícil de estimar en el caso de ataques deliberados, en sistemas o entornos nuevos y ante hechos abstractos.

En general, la estimación de la probabilidad/frecuencia introduce una cierta incertidumbre en detrimento de la credibilidad del análisis de riesgos.

***f) Riesgo / Riesgo residual***

Es el grado de exposición a que una amenaza se materialice sobre uno o más activos, causando daños o perjuicios a una Organización.

Una vez aplicadas las salvaguardas, al entorno del sistema, debería reducirse el riesgo alcanzando el conocido como riesgo residual.

### ***g) Salvaguardas***

Se trata de las medidas de seguridad, procedimientos o mecanismos tecnológicos orientados a reducir el riesgo. Puede tratarse de medidas de previsión o de preparación, de disuasión, protección, detección, aislamiento, confrontación, recuperación, restauración, compensación, etc.

La implantación y la madurez de las salvaguardas disminuye el riesgo, bien reduciendo el impacto causado por una amenaza, o bien la probabilidad o frecuencia de su materialización. Existen modelos como el CMMI (Capability Maturity Model ® Integration) que establecen niveles diferenciados, para representar la existencia y estado de madurez de una salvaguarda

Concepto	Significado
Activo	Elementos que tengan valor
Amenaza	Causa potencial de incidentes
Vulnerabilidad	Debilidades de un activo
Impacto	Consecuencia de un incidente
Probabilidad	Indicador de posibilidad o frecuencia
Salvaguarda	Medio para reducir el riesgo
Riesgo	Posibilidad de sufrir un daño o pérdida

**Figura 2.4 - Resumen de conceptos genéricos implicados en el Análisis de Riesgos**

Un factor a tener en cuenta al realizar un AARR es el nivel de profundidad y el detalle que se propone alcanzar. La definición de activos, por ejemplo, puede ser tan extensa como se quiera, lo cual inevitablemente repercutirá en la complejidad y resultados del AARR. Por ello, se consideran diferentes enfoques que permitan cubrir adecuadamente las necesidades del AARR:

- ***Enfoque de Mínimos:*** En el que se establece una línea base uniforme de seguridad para todos los sistemas, sin establecer distinciones en relación a su criticidad. El AARR examina el estado de seguridad del sistema de información, contra dicha línea base. Dependiendo de lo exigente que sea la línea base, se requerirá un mayor o menor esfuerzo para la realización del AARR, pudiendo resultar excesiva o insuficiente según la criticidad de cada sistema afectado.
- ***Enfoque Detallado:*** En el que se realiza un análisis pormenorizado de todos los sistemas o activos, aumentando la complejidad y el esfuerzo requerido. Su fiabilidad a la hora de detectar los riesgos es mayor, pero pueden diluir la importancia de los sistemas más críticos, al no asignarles una prioridad relativa frente al resto de sistemas.
- ***Enfoque Combinado:*** Tiene en cuenta ambas vertientes analizando a alto nivel el sistema de información, entrando en un mayor detalle para los sistemas críticos, y estableciendo una línea base para el resto. De este modo se optimizan los recursos y el esfuerzo aplicado al AARR.

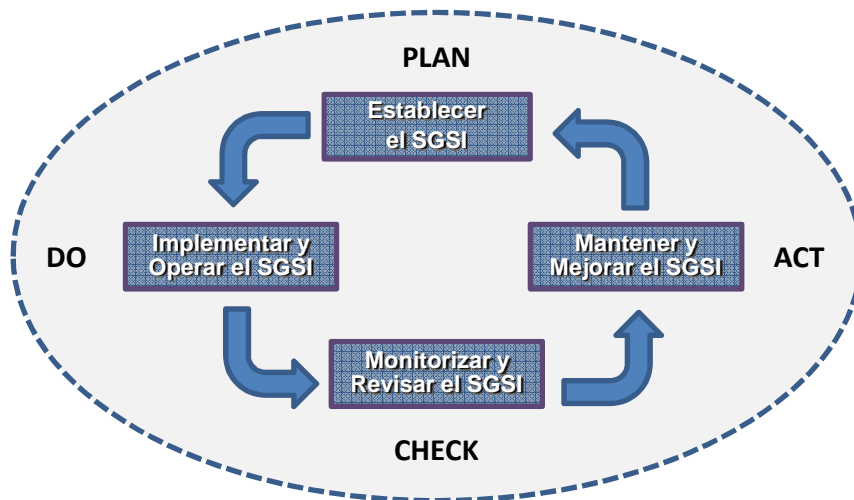
### 3 ANÁLISIS Y GESTIÓN DINÁMICA DEL RIESGO

---

La evolución continua y a gran velocidad de la sociedad tiene su reflejo en los sistemas de información y en el entorno tecnológico en el que se integran. Sobre estos sistemas de información recaen una gran parte de los servicios considerados vitales en la actualidad tanto a nivel civil como militar, así como el tejido industrial, comercial y de ocio que sostienen nuestro estado del bienestar.

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 Gestión del Riesgo 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 [16] 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 (ver *Figura 3.1*). En el caso del National Institute of Standards and Technology (NIST) se contemplan 6 pasos dentro del proceso de gestión del riesgo, que se repiten a lo largo del ciclo de vida del sistema [1].



**Figura 3.1 - Modelo PDCA aplicado al Sistema de Gestión de Seguridad en la Información**

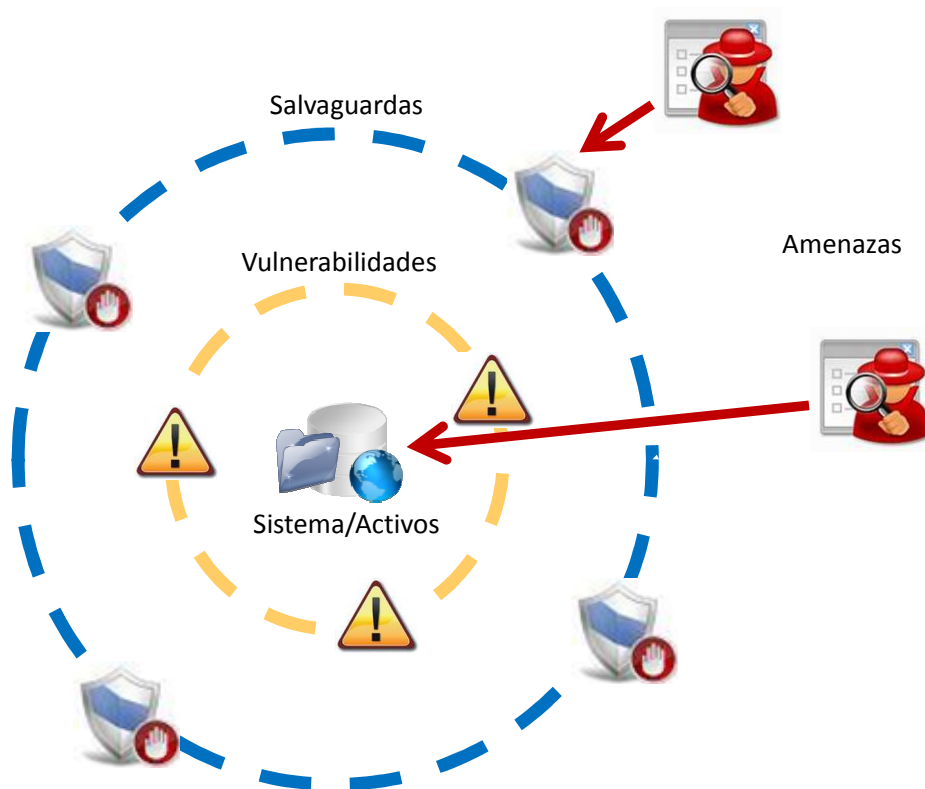
Sin embargo, esta es una falsa percepción de dinamismo ya que la repetición del proceso tiene lugar en intervalos discretos de tiempo y, por pequeños que éstos sean, hay margen para la ocurrencia de cambios que afecten de forma inmediata y crucial al riesgo.

### 3.1 Concepto

La base de una adecuada Gestión del Riesgo se sustenta en la monitorización del riesgo, iterando siempre que sea necesario el proceso de análisis y corrigiendo aquellas desviaciones surgidas (por los motivos expresados anteriormente) en relación a los procesos de AARR previos, tal y como recoge ISO 27005 (ver Figura 2.2).

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 Gestión del Riesgo. Tal y como recoge [18] la línea que delimita la gestión preventiva del riesgo asociada a planes de mitigación del riesgo a corto, medio o largo plazo, se difumina cobrando el matiz de gestión reactiva al pretender reaccionar frente a diferenciales del riesgo, en tiempo real.

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 [18-21]. Éstas se pueden agrupar en 4 grandes conjuntos (ver Figura 3.2):



**Figura 3.2 - Principales variables involucradas en Análisis de Riesgos de Sist. Información**

- ***Cambios en el sistema:*** introducción, alteración o supresión de activos como máquinas, aplicaciones o arquitecturas de red. Este grupo también englobaría las alteraciones en los servicios que dan soporte al sistema, tales como recursos, mantenimientos, proveedores, etc.
- ***Nuevas vulnerabilidades y amenazas*** detectadas y en el peor de los casos, desconocidas.
- ***Evolución de las amenazas conocidas,*** ya sea por eventos y alertas de seguridad detectadas y propagadas por los sistemas de seguridad desplegados, así como el



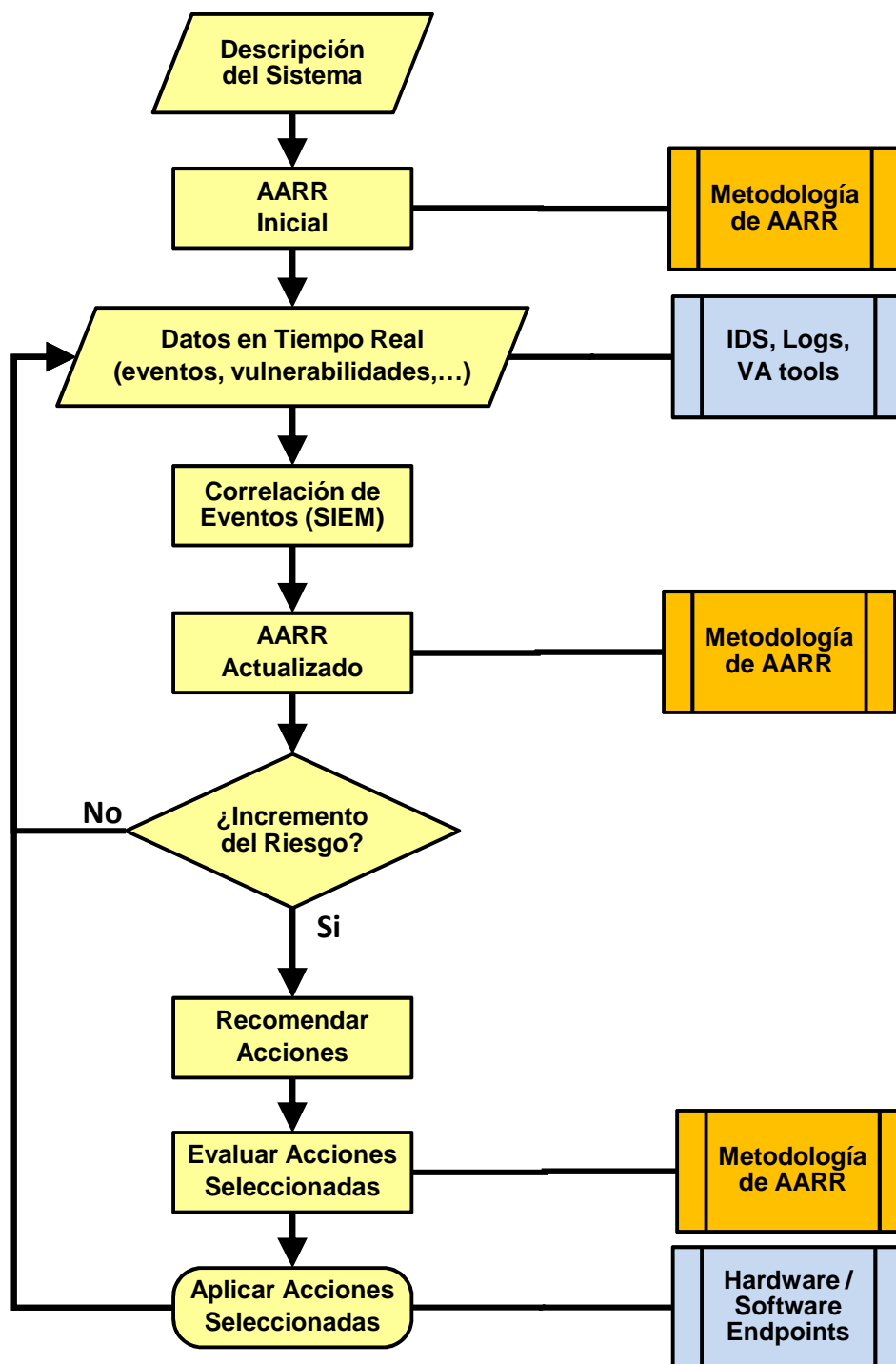
aumento genérico del nivel de riesgo en el entorno, causado por amenazas expresas o previsión de desastres naturales, entre otras.

- *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 [22], 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 gráficamente se recoge en [19] (*ver Figura 3.3*).

En la bibliografía analizada, se utilizan ocasionalmente referencias al “Online Risk Assessment” [23-24] o “Real Time Risk Assessment” [1,24], 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.



**Figura 3.3 - Flujo de un DRA basado en un bucle reiterativo, en base a un AARR estático<sup>4</sup>**

<sup>4</sup> Del original publicado por P. Lagadec en [19]

## **3.2 Objetivos**

Los procesos de AARR y su consecuente gestión, por definición se orientan a facilitar la toma de decisiones sobre tratamiento de riesgos, teniendo en cuenta el binomio coste-beneficio fundamentalmente, de modo que se puedan desarrollar planes de mitigación en base a estas decisiones.

Cabría concebir el AARR Dinámico, yendo un paso más allá de modo que sea posible aportar los siguientes valores añadidos:

- Facilitar la toma de decisiones en tiempo real frente a intrusiones, en base al nivel de riesgo que estas representan a alto nivel, y no limitándose a responder a una alerta aislada emitida por los sistemas de seguridad.
- Reasignar prioridades, en particular a medidas de mitigación que puedan paliar la situación real de riesgo, y que en la elaboración de los Planes de Mitigación pudieran no haber sido contempladas, o haber sido planificadas a medio o largo plazo, atendándose a unos objetivos que podrían resultar actualmente obsoletos.
- Activar/desactivar protocolos, procedimientos o salvaguardas ante variaciones del riesgo en el entorno, de manera proporcional a dicha variación y con prontitud.
- Optimizar o reorganizar los recursos disponibles en tiempo real, de modo que el sistema de información pueda responder a los requisitos de negocio, de la manera más adecuada, pese a los riesgos que lo puedan amenazar.

## **3.3 Evolución del Análisis de Riesgos Dinámico**

En este trabajo 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 que separa unas soluciones de otras.

### ***3.3.1 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 [26] 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 [19] tales como CVE, NVD, CPE, OVAL, KML, CVSS, etc.

Actualmente, existirían diversas bases de datos abiertas para uso público como [27], y especializadas fundamentalmente en la publicación de vulnerabilidades en los sistemas informáticos. También se encuentran en número cada vez mayor [28], iniciativas de gobiernos y consorcios para compartir información, de manera anónima cuando las circunstancias lo requieren, sobre amenazas, vulnerabilidades, intrusiones o anomalías cibernéticas, a través de entidades como CERTs o ISACs.

### ***3.3.2 Grafos y Árboles de ataque***

Este campo enfoca eminentemente el AARR, hacia la evolución que puede seguir una acción intencionada contra el sistema, recogiendo las posibles dinámicas del ataque.

Cuando se habla de seguridad física es fácil asimilar el concepto de defensa en profundidad, consistente en sucesivas capas de protección (fosos, vallas, muros, paredes, cajas de seguridad, etc.) que un atacante debería superar, uno a uno, en caso de querer llegar al objeto preciado que protegen. El razonamiento detrás de los Árboles o Grafos de Ataque es semejante. Con sus peculiaridades, Grafos y Árboles de Ataque [18], 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 dos enfoques:

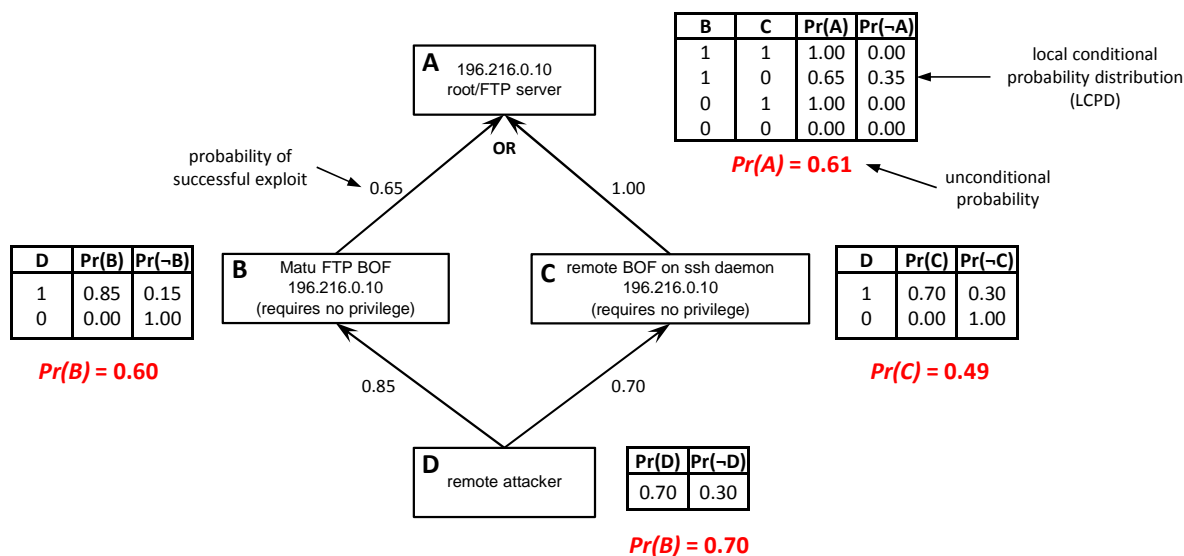
- La simulación de crisis basadas en escenarios de ataque, que permitan emular situaciones reales en un entorno controlado, de cara al entrenamiento del personal técnico y/o directivo.
- A una Gestión Dinámica del Riesgo basada en la respuesta en tiempo real a incidentes de seguridad, que están teniendo 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 pueden ofrecer alarmas y valoraciones en base a factores internos, pero no en base a una metodología de AARR que permita integrar el valor del riesgo, en el contexto global del sistema.

Los cálculos, como ocurre en [18,29<sup>5</sup>], se implementan principalmente mediante Redes Bayesianas que permiten representar, a través de un modelo gráfico (*ver Figura 3.4*), las

---

<sup>5</sup> El artículo hace referencia a un enfoque examinado posteriormente, pero que también incluyen el uso de árboles de ataque.

relaciones probabilísticas entre un conjunto de variables en un grafo acíclico dirigido (DAG). En [30-31] se analiza el uso de Hierarchical Coordinated Bayesian Model (HCBM), para analizar la ocurrencia de eventos extremos, integrando múltiples BBDD de conocimiento sobre amenazas.



**Figura 3.4 - Representación de un grafo de ataque<sup>6</sup>**

Trabajos como [32-33] 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 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 [34]. 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

<sup>6</sup> Del original publicado por N. Poolsappasit en [29]

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.

### **3.3.3 Enfoque mixto**

Las soluciones planteadas previamente se centran en algunos de los aspectos que afectan al cálculo del riesgo en el entorno de los SSII, pero dejan muchos otros aspectos 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 [29] 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 [19] 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.

En el ámbito de los sistemas SCADA (Supervisory Control And Data Acquisition) que permiten la monitorización de las redes que soportan entre otros, los sistemas de gestión de electricidad (EMS) y otras tipologías de las conocidas como Infraestructuras Críticas, la gestión en tiempo real del riesgo se ha venido desarrollando desde tiempo atrás. En el caso de [35] esta gestión “on-line” ha sido aplicada desde el punto de vista de la operativa, en relación a caídas de voltaje en redes de distribución eléctrica.

### ***3.3.4 Monitorización de estado del sistema***

La tendencia actual en gestión de seguridad en SSII es la tecnología SIEM [36] 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 o predecir en tiempo real trazas de actividad maliciosa dirigidos contra la red y sus recursos.

El conocimiento de dichas actividades detectadas por los IDS/IPS, además de ser explotado por los árboles de ataque para determinar el grado de avance del atacante y las probabilidades de que alcance un posible objetivo final (conforme se explica en apartados anteriores), puede ser alternativamente 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 [24] 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 [37]. 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 [23] 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) [38] 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 [25] 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 su aplicación en aspectos más 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 [20] 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 los modelos estadísticos bayesianos para el cálculo y transmisión de las 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 otros casos, como en [39] 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.

### **3.4 Evolución del Tratamiento Dinámico del Riesgo**

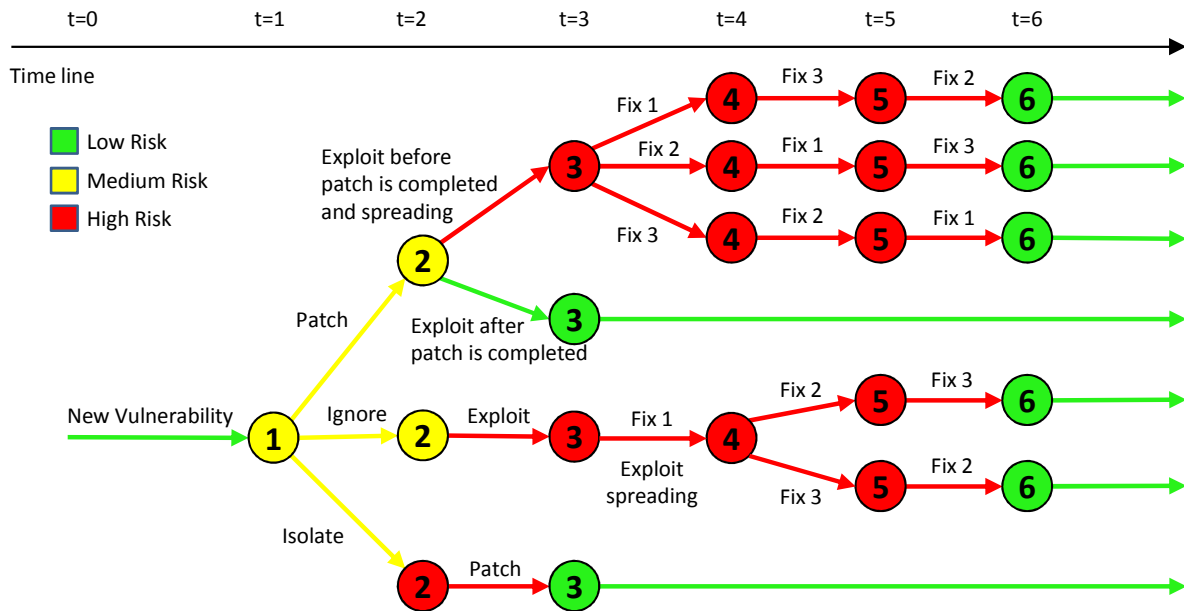
La ventaja que un AARR Dinámico plantea frente al modelo fuertemente implantado de análisis estático, es la de una gestión también dinámica, del riesgo en tiempo real, que permita el tratamiento del riesgo respondiendo con las salvaguardas más adecuadas allá donde se manifieste realmente éste. Del mismo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

#### ***3.4.1 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 el sistema de información 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 [21] ante una nueva vulnerabilidad el árbol recorre las

posibles acciones alternativas que permitirían paliarla, asumiendo el menor riesgo posible (ver Figura 3.5).



**Figura 3.5 - Árbol de optimización de tratamiento de vulnerabilidades por riesgo<sup>7</sup>**

La generación de estos árboles requiere de un proceso de aprendizaje supervisado (Reinforcement Learning), basado en la aplicación de Redes Neuronales conforme se detalla en [40].

### 3.4.2 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 [23] 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.

<sup>7</sup> Del original publicado por L. Beaudoin en [21]

En [41] se presenta el método RheoStat, 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. Algunos esfuerzos como [42] se centran en intentar 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.

### **3.5 Áreas de Mejora Observadas**

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 principalmente) aportan una visión del riesgo poco generalista y no alineada con las metodologías de riesgo que se emplean normalmente para una 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 de obtener información continua que realmente 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 las herramientas que implementen las metodologías de AARR. Estos datos deberían ser adecuadamente filtrados por las herramientas de seguridad antes de su envío de modo que la herramienta de AARR 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.

## 4 COMUNICACIÓN DE EVENTOS DE SEGURIDAD PARA ANÁLISIS DE RIESGOS DINÁMICO

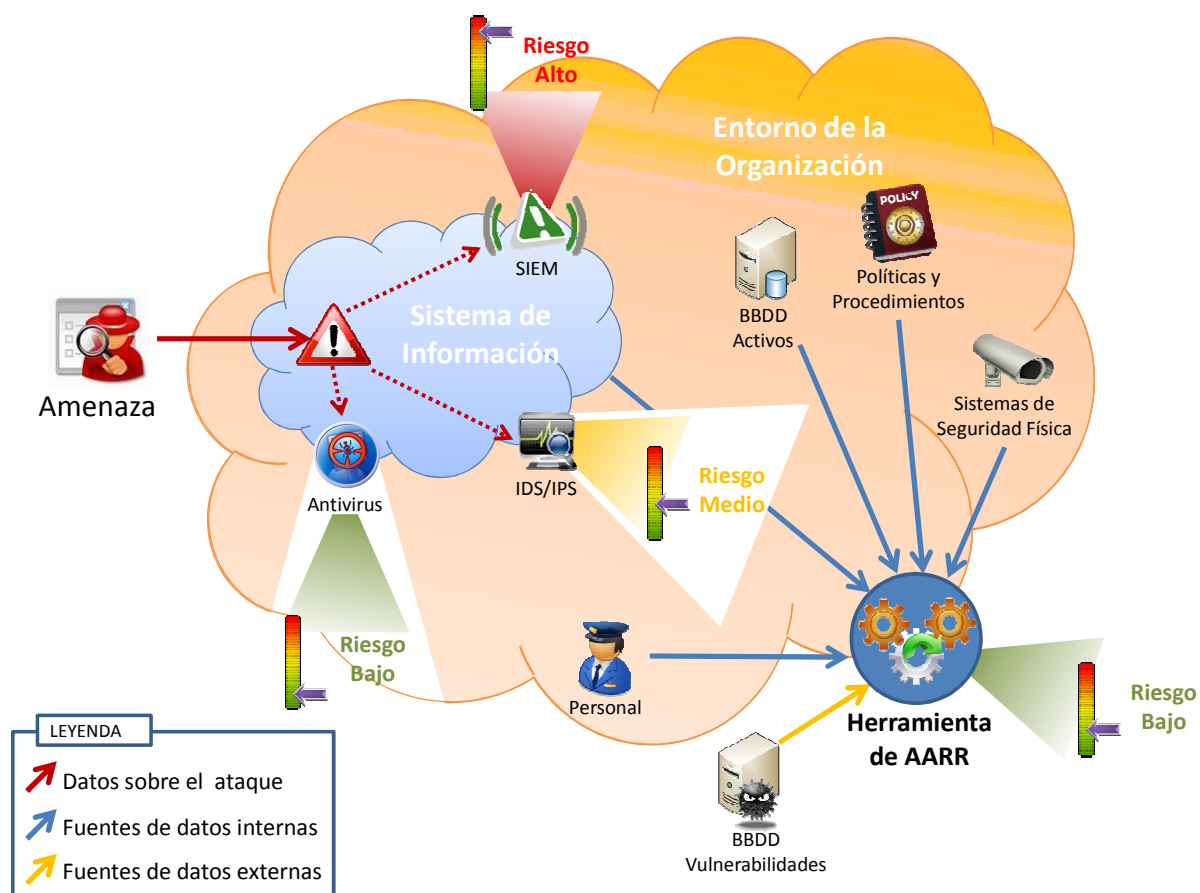
---

Conforme se ha venido presentando a lo largo del Análisis del Estado del Arte previo, en relación al AARR Dinámico, se observa por un lado una patente segregación entre las herramientas de seguridad generalmente implantadas en los entornos TIC y los procesos de AARR ejecutados en las Organizaciones, y por otro el uso no uniforme de modelos de evaluación del riesgo.

La primera afirmación implica que los procesos de AARR que implementan metodologías ampliamente reconocidas (*ver el Capítulo 2 Introducción al Análisis y a la Gestión del Riesgo*) no se alimentan directamente de la importante fuente de información que suponen las herramientas de seguridad (Firewalls, IDS/IPS, antivirus, SIEM, etc.) ni de manera estática a modo de BBDD con información histórica, ni mucho menos en tiempo real, lo que permitiría una evaluación del riesgo inmediata frente a ataques en curso.

La segunda afirmación se hace patente por el hecho de que las herramientas, cuando disponen de capacidades para ello, utilizan modelos propios para el cálculo de la criticidad o niveles de riesgo que determinados eventos de seguridad implican, no aplicando metodologías reconocidas, ni los criterios alineados/uniformes con los objetivos del negocio que una Organización busca reflejar en sus correspondientes procesos de AARR (*ver Figura 4.1*).

A este respecto las herramientas más completas tienden a ser las SIEM (Security Information Event Management) que realizan una valoración del riesgo considerando diversos factores como: activos hardware que componen el sistema, algunas fuentes de información sobre vulnerabilidades y eventos de seguridad. Sin embargo, ofrecen una visión del riesgo limitada frente a la obtenida de un AARR metodológico y basado en un ámbito más extenso de la organización que el ceñido exclusivamente al propio Sistema de Información.



**Figura 4.1 - Evaluación del Riesgo NO integrada**

## 4.1 Motivación de la Propuesta de Trabajo

La realización de un AARR para los Sistemas de Información de una Organización es un trabajo que requiere un esfuerzo sustancial, y que incluye la recopilación de una importante cantidad de datos sobre la estructura y activos de la información, sus interrelaciones y las amenazas que los acechan. Hasta el momento, esta inversión de trabajo tiende a utilizarse puntualmente como el punto de partida para la definición de un Plan de Mitigación de Riesgos a diferentes plazos, renovándose el resultado del AARR periódicamente, en el mejor de los casos transcurrido un lapso de tiempo considerable.

Puesto que los SSII, y del mismo modo los riesgos sobre éstos, evolucionan a gran velocidad el anterior planteamiento implica que el esfuerzo invertido puede quedar desfasado, si no se realiza un adecuado seguimiento y actualización continuada del AARR. El ejemplo más extremo en este sentido, ocurre durante la materialización de una amenaza en lo que catalogaríamos como un incidente de seguridad, que bien de manera puntual o durante un periodo de tiempo en función de la evolución del incidente, altera por completo el panorama del riesgo desvirtuando, al menos temporalmente, los resultados de los AARR previos.

Por esta razón, se plantea como foco de análisis el hecho de que una adecuada comunicación entre las herramientas dedicadas a monitorizar las redes en tiempo real (capaces de detectar la ocurrencia y evolución de determinados incidentes de seguridad) y aquellas utilizadas para realizar un AARR, permitiría:

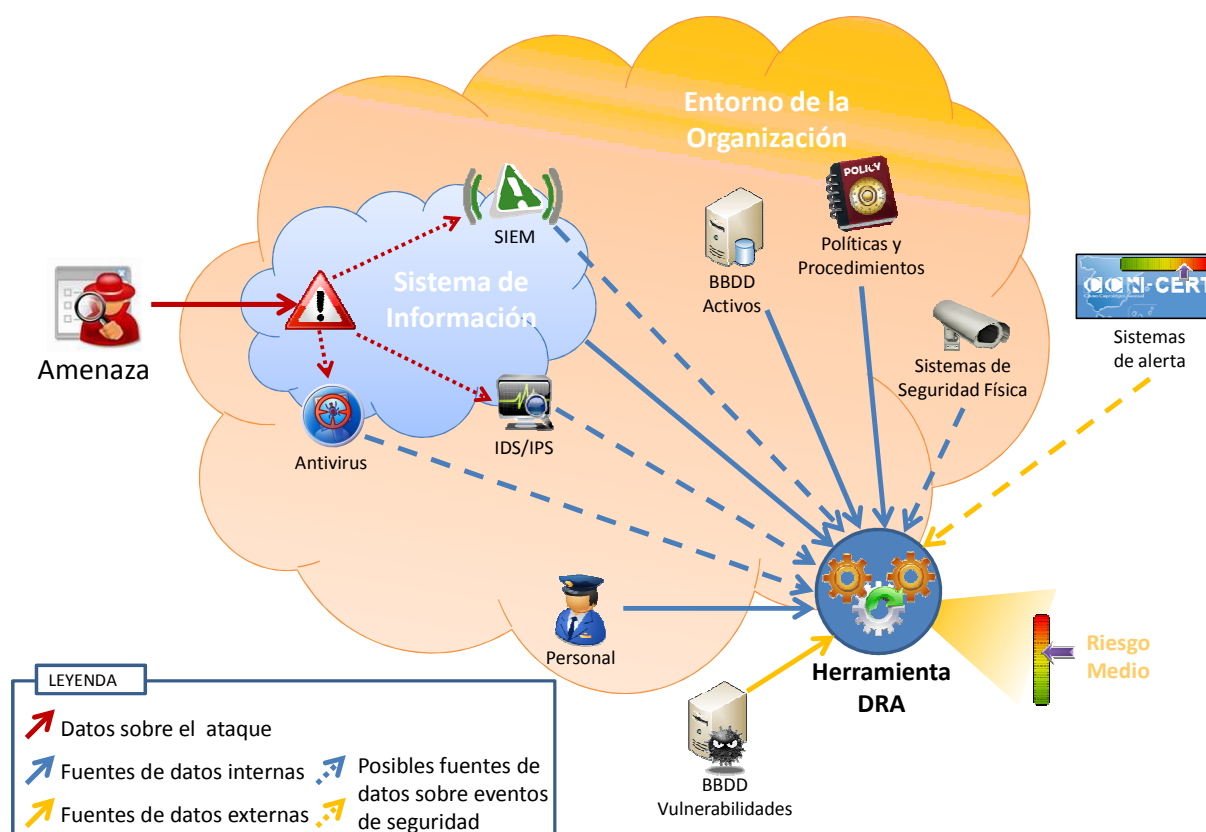
- Contar con capacidad para la monitorización en tiempo real del AARR, que facilite la construcción o actualización de árboles y grafos de ataque, permitiendo conocer el riesgo real para los activos críticos.
- Disponer de un cuadro de mandos sobre el riesgo, actualizado de manera instantánea, que además refleje el nivel de riesgo de manera uniforme y homogénea con los procesos de AARR estáticos desarrollados por la Organización. En este ámbito se incluyen las dependencias existentes de activos de nivel superior (i.e. Datos o Servicios) que pueden ser reflejados a través de procesos metodológicos de AARR frente a soluciones ad-hoc de menor amplitud.

En trabajos previos orientados a un enfoque semejante como ocurre en [42], se contempla el cálculo centralizado del riesgo en base a un proceso de filtrado de las alertas, detectadas básicamente por los dispositivos IDS desplegados en una red. Este proceso de filtrado se orienta en las tres fases sucesivas que lo componen, a fusionar las alertas provenientes de múltiples IDS dentro de un mismo contexto, a identificar las amenazas que originan las alertas, y finalmente a integrar el riesgo desde un punto de vista global. Como se observa en otros trabajos, el riesgo es calculado en base a una metodología ad-hoc, en lugar de apoyarse en estándares o metodologías



ya establecidas. En [43] se contempla el uso de una adaptación de la metodología MEHARI, que permita su integración con una red de IDS orientada a determinar automáticamente acciones reactivas en función del nivel de riesgo. Del mismo modo, herramientas como los productos SIEM ejecutan una importante labor de centralización e interpretación de los eventos de seguridad detectados en una red, abordando la tarea de filtrar y dar sentido a estos eventos (*ver Figura 4.2*).

Es en el punto intermedio, en la comunicación entre una herramienta de detección y análisis de incidentes, y una herramienta especializada en el AARR en base a una metodología, donde existiría una problemática de interconexión. Existen intentos de estandarizar formatos de datos relacionados con la comunicación de incidentes de seguridad o eventos de intrusión, pero no enfocados al ejercicio planteado, sino principalmente a la compartición de incidentes entre CERTs o CSIRTs, como se verá a continuación.



**Figura 4.2 - Evaluación del Riesgo Integrada**

## 4.2 Modelos de Datos Relacionados con la Gestión de Incidentes

Conforme a [44], se definen respectivamente:

- Evento de seguridad de la información: La ocurrencia detectada en un estado de un sistema, servicio o red que indica una posible violación de la política de seguridad de la información, un fallo de las salvaguardas o una situación desconocida hasta el momento y que puede ser relevante para la seguridad.
- Incidente de seguridad de la información: Un único evento o una serie de eventos de seguridad de la información, inesperados o no deseados, que tienen una probabilidad significativa de comprometer las operaciones empresariales y de amenazar la seguridad de la información.

La comunicación y compartición de datos sobre incidentes de seguridad ha sido foco de atención por parte de organismos de estandarización como el Internet Engineering Task Force (IETF), quién a través de su Grupo de Trabajo Extended Incident Handling (INCH WG) han realizado esfuerzos para estandarizar los flujos de información en relación a incidentes de seguridad.

Estos intentos por estandarizar la manera de intercambiar información relativa a incidentes de seguridad, se han enfocado en primer lugar, al intercambio de información sobre intrusiones en SSII a través del protocolo experimental IDMEF [45], para ampliarse posteriormente hacia un formato para el intercambio de información sobre incidentes bajo el nombre de IODEF [46], fundamentalmente orientado a la cooperación entre equipos de respuesta frente a incidentes de seguridad (más conocidos como CERT o CSIRT).

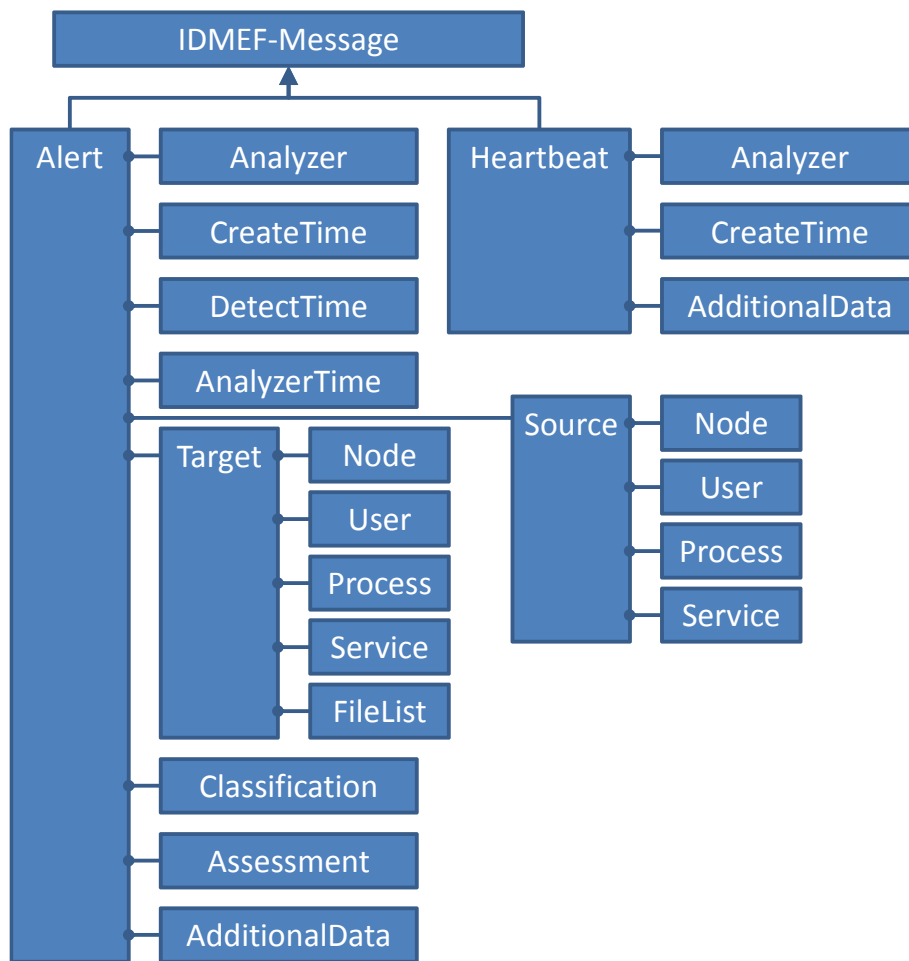
### 4.2.1 *Intrusion Detection Message Exchange Format (IDMEF)*

El propósito de IDMEF es definir formatos de datos, independientes del protocolo de comunicación, que junto a procedimientos de intercambio apropiados proporcionan un marco para la comunicación de información relativa a intrusiones en SSII. Esta comunicación tiene lugar entre sistemas de detección y respuesta, y sistemas de gestión que requieran interactuar con ellos.

Es común que las intrusiones afecten, bien a diferentes organizaciones como objetivos o víctimas, bien a múltiples entornos dentro de una misma organización bajo cobertura de distintas tecnologías de IDS, por lo que sería de utilidad poder tratar toda la información generada al respecto, en su conjunto para producir resultados más clarificadores.

Actualmente el formato se encuentra en fase experimental sometido a comentarios en 2007, a través del RFC4765 [45] del mismo modo que los procedimientos que lo complementan. Dicho RFC propone un modelo de datos para la representación de información a ser exportada y comunicada automáticamente por un IDS, ante la detección de eventos sospechosos, junto con una implementación en XML y ejemplos de uso. El modelo persigue facilitar la notificación tanto de eventos simples de seguridad, como aquellas más complejas que surgen de la correlación de múltiples eventos.

El modelo se basa en clases jerárquicamente asociadas a una instancia de un mensaje IDMEF, existiendo dos tipos de mensaje, las alertas y las notificaciones de estado (Heartbeat). Los IDs integrados en una arquitectura con un elemento destinado a la monitorización, generarían periódicamente mensajes Heartbeat para notificar a dicho sistema de monitorización su actividad, mientras que emitirían mensajes de Alerta cuando un evento de seguridad contemplado en las políticas al efecto lo justificase. La estructura de datos, recogida conforme a [47] se representa en la *Figura 4.3*.



**Figura 4.3 - Modelo de Datos IDMEF**

Las clases que componen el núcleo de los mensajes IDMEF, son las encargadas de identificar el objetivo contra el que se dirige el evento de seguridad detectado y el origen desde el que se genera el evento, en caso de ser conocidos, y que da pie a la alerta. Esta identificación se realiza a nivel de nodo de red, usuarios, procesos o servicios.

Los mensajes contienen también información sobre el componente del IDS que detectó el evento y/o generó el mensaje, junto con registros de tiempo. Se incluye una Clasificación del evento en caso de disponerse de una categoría identificable, bien de listas estandarizadas o bien específicas de la distribución del IDS para eventos particulares y no estandarizados, así como una evaluación del posible impacto que el evento detectado podría suponer sobre el objetivo.

Finalmente, el formato habilita una clase para añadir información adicional que no encaja en las anteriores clases pero que podría facilitar información importante de cara a la comprensión y análisis del evento, proporcionando la posibilidad de extender el formato IDMEF.

El formato ha sido asimilado en el entorno de los proveedores de herramientas IDS, si bien no permite tratar adecuadamente información sobre incidentes en un contexto más general como se apunta en [48].

#### ***4.2.2 Incident Object Description and Exchange Format (IODEF)***

Define una representación de datos, que proporciona un marco para la comunicación de información relativa a incidentes de seguridad en SSII, comúnmente compartida entre Equipos de Respuesta a Incidentes (CSIRTs) con una finalidad operativa y estadística. Adicionalmente, se concibe con la intención de proporcionar un fundamento para el desarrollo de herramientas interoperables y procedimientos de notificación de incidentes.

Los incidentes de seguridad en la actualidad, pueden involucrar múltiples sistemas de información en diferentes dominios, bajo supervisión de sus respectivos CSIRTs. La colaboración efectiva entre ellos, a través de estándares apropiados tal y como recoge [49], resulta vital de cara a una adecuada resolución de estos incidentes, si bien cada equipo contará con sus propios sistemas, formatos y procedimientos para la gestión de los incidentes.

El grupo de trabajo al cargo del desarrollo de este formato entre 2002 y 2008, inicialmente el IODEF Working Group y posteriormente retomado por el IETF Extended Incident Handling (INCH) Working Group, tenía por objetivo definir formatos orientados a la comunicación entre:

1. CSIRTs y colaboradores implicados en la notificación de abusos de los SSII.
2. Los propios CSIRT y el resto de actores implicados en la investigación de incidentes.

### 3. Diferentes CSIRT colaborando y compartiendo información relativa a los incidentes.

Para ello, se requería [50] que el formato permitiese la acumulación progresiva de información inherentemente heterogénea, a lo largo de las diferentes fases de investigación que constituyen el ciclo de vida del incidente, desde la notificación inicial fuera cual fuese su fuente originaria (CSIRT, comunidad de usuarios, IDS, etc.), hasta su resolución, recopilada y agregada en el tiempo por los CSIRTs sucesivamente involucrados. Fundamentalmente, esta información debía centrarse en definir el origen y el objetivo del incidente, así como características sobre su comportamiento, evidencias que soportaran los resultados y conclusiones, junto con el diseño del proceso de investigación.

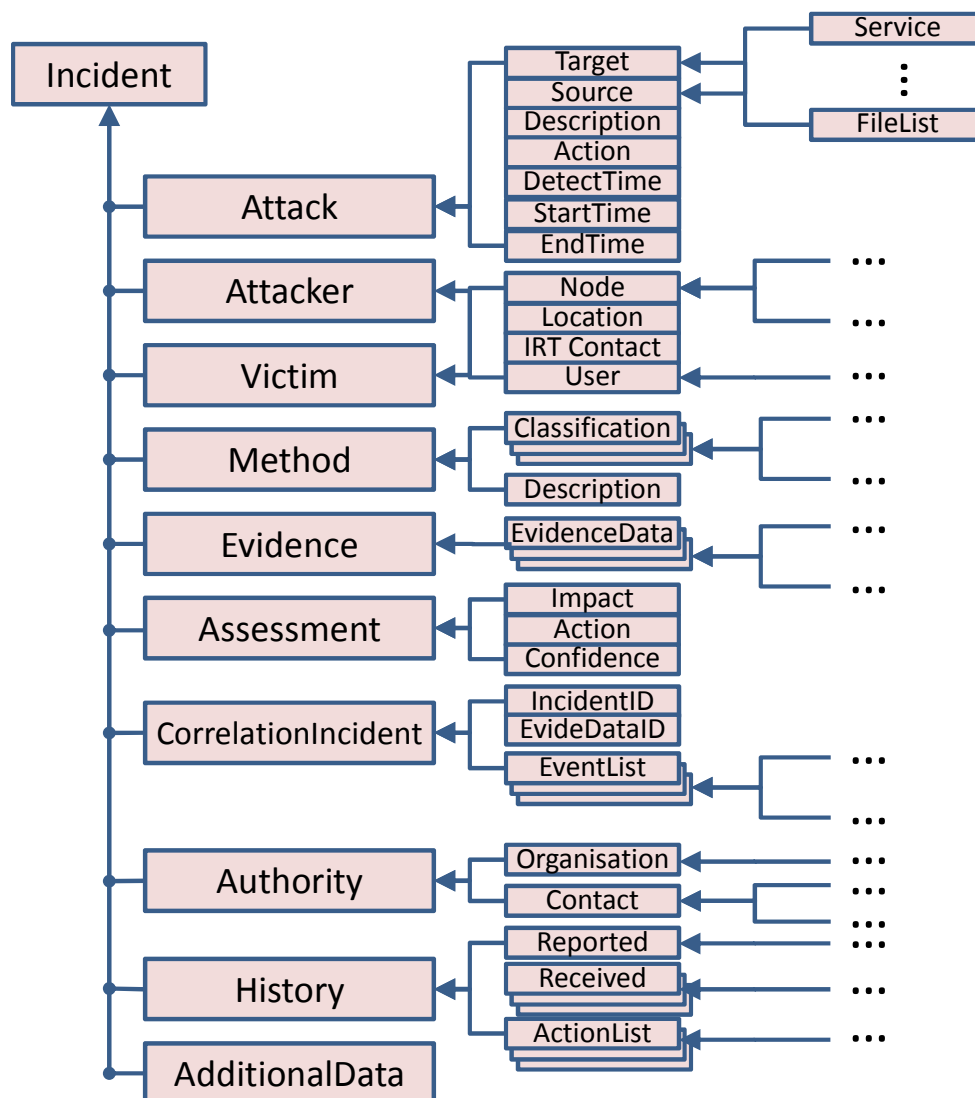
Uno de los principios de diseño aplicados a IODEF [51] es el de que fuera compatible con el formato IDMEF, de modo que el subconjunto de incidentes que representan los intentos de intrusión detectados por los sistemas IDS, pudiera tener cabida en el nuevo formato. Es por ello que la terminología utilizada por IODEF extiende la de IDMEF, aunque existen diferencias fundamentales entre ambos como muestra [50], entre las que destacan que:

- IODEF es un modelo orientado principalmente a la comprensión e interacción humana, si bien, ofreciendo siempre la posibilidad del tratamiento automatizado (parseado o análisis sintáctico de las estructuras de datos) por parte de sistemas de información.
- Las estructuras de datos de IODEF deben facilitar la gestión de un ciclo de vida mucho más complejo, que el de los mensajes de usar y tirar, de modo que puedan ser manejados como parte de informes, investigaciones, etc., almacenados coherentemente, y que permitan la generación de estadísticas o el estudio de tendencias.

Adicionalmente, el formato contempla la existencia de metadatos para representar detalles relativos al intercambio de información de seguridad entre dominios administrativos, que

incluyen niveles de confianza (o certeza) sobre la información transmitida, aspectos de internacionalización, sensibilidad y restricciones de uso sobre los datos.

El potencial de IODEF permitiría que la información compartida sea relativa a incidentes conocidos, o bien a nuevas tipologías de éstos. Al igual que en IDMEF, el modelo IODEF se basa en clases jerárquicamente asociadas a una instancia de un incidente, que en sus versiones iniciales de 2002 [52] elaboradas por el IODEF WG con apoyo de la Trans-European Research and Education Networking Association, comprendían los siguientes aspectos (*ver Figura 4.4*):

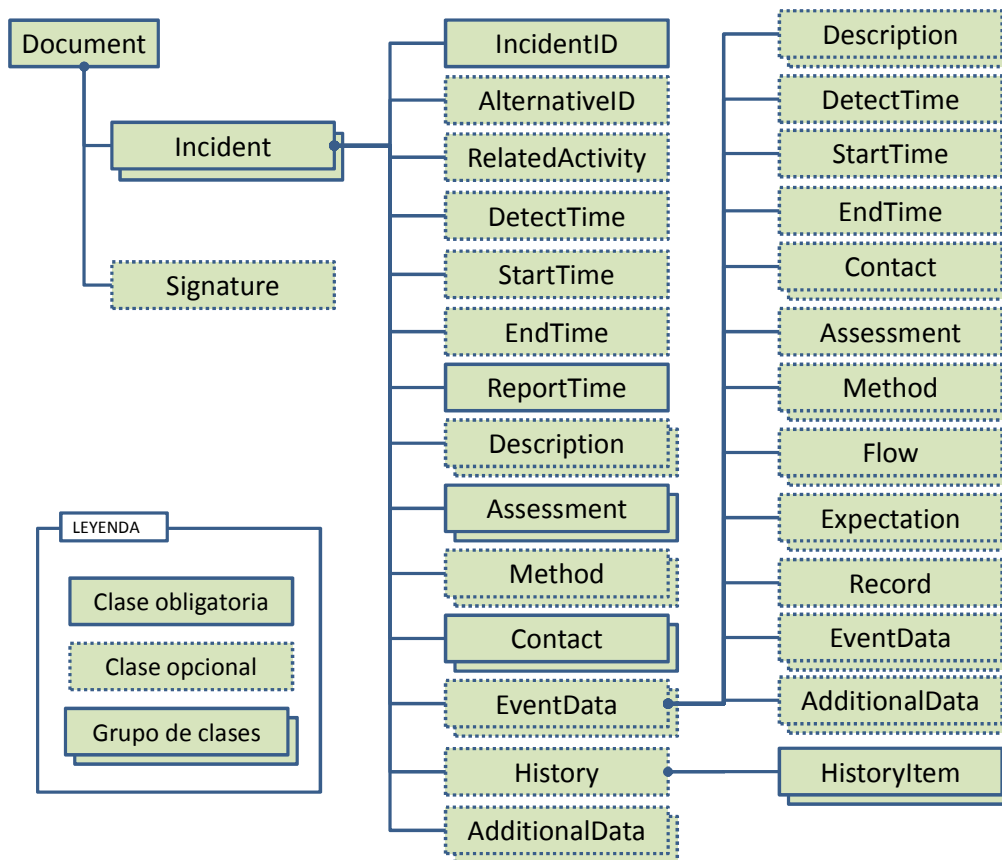


**Figura 4.4 - Modelo de Datos IODEF (versión inicial del IODEF WG)**

Las estructuras de datos disponen de una configuración anidada en múltiples niveles (hasta 7 a priori), lo que permite plasmar un gran nivel de detalle en la definición y seguimiento de los incidentes, disponiendo también como ocurría en IDMEF de una clase para añadir información adicional, orientada a proporcionar la posibilidad de extender el formato. De hecho, algunas de las clases susceptibles de requerir el movimiento de grandes volúmenes de datos asociados, como las referidas a listados de datos sobre históricos y evidencias. Las clases Incident, Attacker, Evidence, Victim, Source, Target, Node, User, Process, Service, Address, y UserID disponen de un atributo identificativo que en caso de rellenarse debe tener un valor único para todas las instancias de incidente creadas por un organismo en particular.

Como se recoge en [53] el modelo era en exceso complejo y con demasiados elementos obligatorios. Posteriormente, fue evolucionando en sucesivas fases de RFC, hasta disponer de una estructura alejada de la inicialmente diseñada [46] y basada en unas listas más reducidas de atributos y sustancialmente más genéricas, de modo que facilite el modelado de estructuras de datos más amplias y diferenciadas (*ver* Figura 4.5).





**Figura 4.5 - Modelo de Datos IODEF (versión final del IODEF INCH)**

En este caso un Documento IODEF puede aglutinar la información de varios incidentes, que requieren contar obligatoriamente con datos relativos a su identificación, momento en que fueron detectados o comunicados, evaluación del incidente, así como datos de contacto relevantes. El resto de datos son opcionales, siendo también posible anidar algunas de las clases (como la propia evaluación o datos de contacto) de modo que se enriquezca la variedad y completitud de los datos.

Al igual que en IDMEF se ha contemplado la posibilidad de extender el modelo añadiendo estructuras para datos adicionales. Este potencial ha sido explotado para desarrollar extensiones más específicas, en particular se encuentran en estado de RFC:

- Una clase para el reporte de eventos sobre fraude mediante Phishing [54], cubierta por el RFC 5901 del IETF.

- La clase para el rastreo de tráfico relacionado con ataques transmitido entre diferentes redes [55], cubierta por el RFC 6045 del IETF.

Si bien se encuentran ejemplos para uso libre, de herramientas desarrolladas para el uso de CERTs/CSIRTs<sup>8</sup>, en [48] se plantea el hecho de que es un modelo en exceso complejo, por lo que no habría llegado a una fase de adopción en masa, resultando fuera del alcance de muchos CERTs la posibilidad de desarrollar herramientas totalmente compatibles con el modelo de IODEF.

### **4.3 Extensión de un Modelo de Datos para Comunicación de Eventos de Seguridad Enfocados al Análisis de Riesgos Dinámico**

Con la intención de aprovechar el esfuerzo acometido para llevar el modelo IODEF a un estado de madurez considerable, y de la ambición de establecerse como estándar para comunicación de incidentes de seguridad, se toma como referente, para el desarrollo de un modelo de datos específico para la transmisión de información relevante de cara al uso por sistemas de AARR metodológicos desplegados en una Organización. Dicha información debería ser en cualquier caso, adecuadamente filtrada por las herramientas de seguridad antes de su envío de modo que la herramienta de AARR Dinámico no se vea saturada de información irrelevante.

El potencial de extensión que aporta IODEF, demostrado en los ejemplos recogidos en el apartado previo, permite encarar la tarea de contemplar el ámbito generalista de incidentes gestionados por sistemas de seguridad aquí planteado, sin que suponga una ruptura con dicho modelo.

La extensión propuesta tomará en consideración la obligatoriedad de completar las clases que el modelo IODEF dispone como imprescindibles, estableciendo nuevas clases a contemplar

---

<sup>8</sup> The European CSIRT Network solutions: <http://www.ecsirt.net/service/products.html>

dentro de la estructura de datos. El resto de clases definidas por IODEF podrán ser opcionalmente completadas, si bien, no serían un requisito para el correcto tratamiento por parte de interfaces de AARR que se adhirieran al modelo presentado.

Tal y como se definió anteriormente y conforme a [44], se considerará el incidente de seguridad como un evento o conjunto de éstos, susceptibles de ser notificados a la herramienta de AARR, contrastados por los sistemas de seguridad desplegados y que inciden en la probabilidad de comprometer la seguridad de la información y por ende, de las operaciones.

La referencia a sistemas de seguridad desplegados, no contempla exclusivamente los sistemas IDS, IPS o SIEM habitualmente implantados para la monitorización de actividades intrusivas. En este modelo, se contemplan como fuentes de información adicionales:

- Los sistemas capacitados para detectar código malicioso, como pueden ser antivirus o anti-malware.
- Los sistemas de gestión de seguridad física capaces de detectar intrusiones u otros incidentes, que tengan lugar en dependencias o protecciones físicas relacionadas con los SSII.
- Los propios CERTs con los que exista colaboración y que puedan facilitar información sobre determinadas situaciones de riesgo a contemplar, si bien más genéricas que las aportadas por los sistemas imbricados en la defensa del Sistema de Información.

Debido a las implicaciones para la seguridad, que la información transmitida sobre estos eventos puede llevar asociada, las comunicaciones deben apoyarse en protocolos de transporte que aseguren medidas de confidencialidad e integridad adecuadas, en especial si la transmisión se produce entre diferentes redes. Conforme a [48] deberían utilizarse protocolos de comunicación que pese a ser seguros no incidan negativamente en el rendimiento, requiriendo excesivos recursos o retardos, durante su gestión automatizada.

Como parte del evento de seguridad, se ven involucrados los siguientes factores que afectan a la evolución del riesgo, conforme a las metodologías de AARR revisadas como parte de este trabajo:

***Activo afectado (AffectedAsset):***

Sería un nuevo atributo encargado de identificar el activo, de entre aquellos contemplados en el AARR, sobre el que impactaría en primera instancia el incidente de seguridad. A través de este atributo podrían identificarse mediante código alfanumérico compartido con la herramienta de AARR, aquellos activos susceptibles de sufrir un ataque.

***Amenaza detectada (DetectedThreat):***

Sería un nuevo atributo que reflejaría el tipo de amenaza relacionada con el ataque observado, en caso de que el sistema que notifique el evento sea capaz de establecer una relación entre ambos parámetros. Las amenazas a considerar podrían partir de un catálogo común con la herramienta de AARR.

***Vulnerabilidad explotada (ExploitType).***

Sería un nuevo atributo que dependiendo del ámbito de vulnerabilidades contempladas se podría recurrir a formatos estándar, tales como CVE, NVD, OVAL, etc.

***Estado de seguridad (SecurityState):***

Sería un nuevo atributo para definir la situación de avance en la que se encuentra el ataque o evento de seguridad, con la finalidad básica de conocer si el sistema de seguridad ha sido superado o aún mantiene al atacante bajo control, pese a que el ataque haya podido tener éxito en cierta medida.

***Sistema notificador (ReportingSystem):***

Sería un nuevo atributo que identificaría el tipo de sistema que ha notificado el evento de seguridad. Dependiendo del ámbito elegido, este podría ir desde IDs/IPs a sistemas de detección de intrusión física o CERTs colaboradores.

***Evaluación (Assessment):***

Esta clase nativa de IODEF pasaría a ser obligatoria, recogería la evaluación general del evento a través de sus componentes relativos al impacto y certidumbre, identificados a continuación.

***Impacto provocado (Impact):***

Esta clase nativa de IODEF pasaría a ser obligatoria, colgando de la clase Assessment que también debería aparecer como atributo asociado al evento. Permitiría definir a través de sus atributos asociados la severidad y estado de consumación del ataque, estimados por el sistema de seguridad que detectó y transmitió el evento.

***Nivel de certidumbre (Confidence):***

Esta clase nativa de IODEF también dependiente de Assessment, pasaría a ser igualmente obligatoria. El sistema de seguridad facilitaría una evaluación relativa a la probabilidad de que la notificación sea debida a un falso positivo. En caso de no disponer de capacidad para determinarla se debería especificar por defecto con un valor de certidumbre que no provoque su descarte por parte de la herramienta de AARR. En caso de observarse un encadenamiento de eventos de seguridad el nivel de certidumbre de las nuevas notificaciones sería consecuentemente mayor.

***Tiempo de detección (DetectTime):***

Esta clase nativa de IODEF dependiente de EventData, pasaría a ser obligatoria. Permitiría establecer en formato unificado el instante de tiempo en que se detectó el evento.

El incidente de seguridad, considerado por IODEF como la clase superior que recogería múltiples eventos, haría referencia a los siguientes factores:

***Identificador del incidente (IncidentID):***

Esta clase nativa de IODEF obligatoria por defecto, permitiría identificar unívocamente el incidente de seguridad.

***Tiempo de notificación (ReportTime):***

Esta clase nativa de IODEF obligatoria por defecto, permitiría establecer en formato unificado el instante de tiempo en que se notificó el incidente por parte del sistema correspondiente.

***Evaluación (Assessment):***

Esta clase nativa de IODEF obligatoria por defecto, recogería la evaluación general del incidente de manera semejante a lo definido para los eventos individualizados. En caso de notificarse un único evento como parte del incidente, la evaluación sería idéntica a la del evento, para los atributos de impacto y certidumbre.

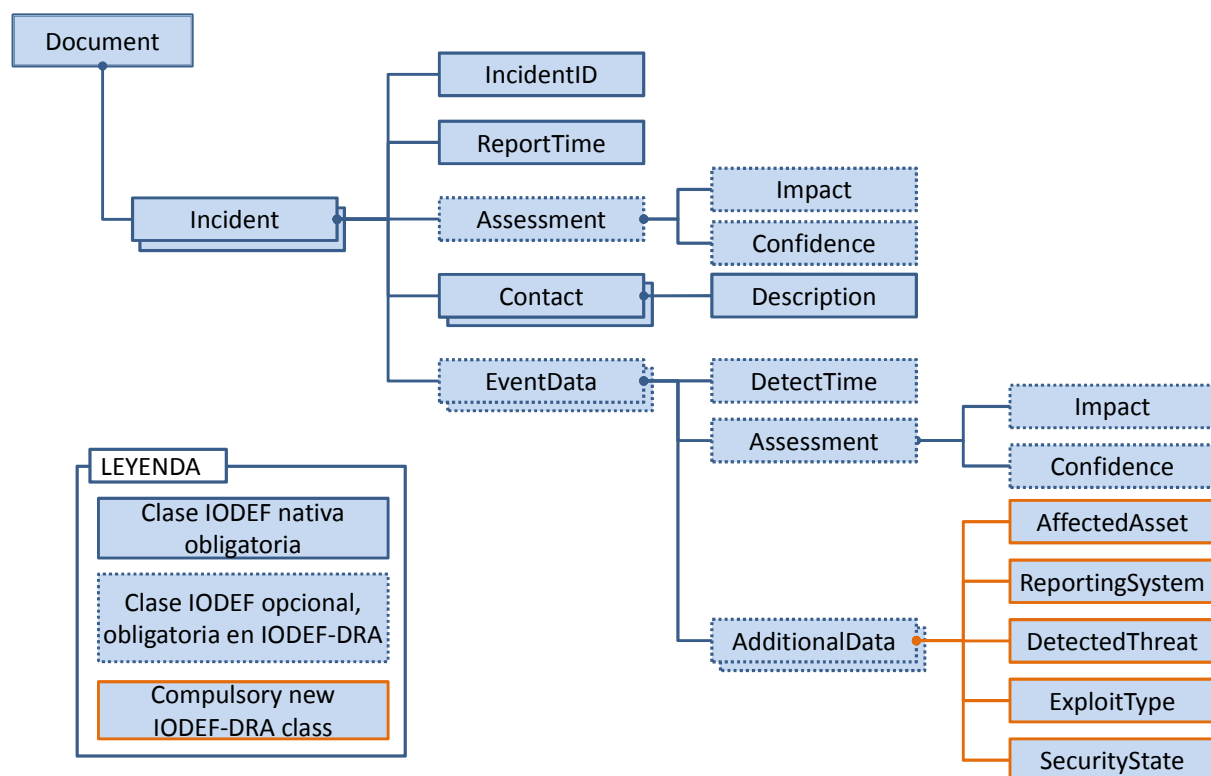
***Información de contacto (Contact):***

Esta clase nativa de IODEF obligatoria por defecto, recogería los datos de contacto del administrador del sistema de seguridad notificador.

***Datos de evento (EventData):***

Esta clase nativa de IODEF opcional por defecto pasaría a ser obligatoria, integrado por uno o una lista de eventos de seguridad conteniendo la información definida previamente.

El formato extendido propuesto conforme las especificaciones anteriores, se reflejaría en la *Figura 4.6*, obviando las clases opcionales del formato IODEF, que no son extendidas por el nuevo formato.



**Figura 4.6 - Modelo de Datos IODEF extendido para AARR Dinámico (IODEF-DRA)**

El diseño de las clases del formato nativo IODEF, involucradas en este modelo, se definen a lo largo de [46]. A continuación, se adjunta el diseño de las nuevas clases contempladas como parte de la extensión para el modelo IODEF-DRA:

- Clase AFFECTED ASSET

- Se compondría de los atributos:

```

STRING type
STRING assetID

```

- Los atributos representarían:

type: sería opcional e identificaría la naturaleza del activo afectado.

`assetID`: sería obligatorio y recogería el identificador unívoco correspondiente al activo particular protegido por el sistema de seguridad y afectado por el evento a notificar.

- Clase REPORTING SYSTEM

- Se compondría de los atributos:

```
STRING type
STRING systemID
```

- Los atributos representarían:

`type`: sería obligatorio e identificaría la naturaleza del sistema que detectó el evento de seguridad.

`systemID`: también obligatorio, recogería el identificador unívoco correspondiente al sistema, de modo que se puedan conocer las características de éste, sus niveles históricos de falsos positivos, e incluso las salvaguardas que pudiera ofrecer, en caso de un desarrollo ulterior de posibles respuestas automatizadas.

- Clase DETECTED THREAT

- Se compondría de los atributos:

```
STRING type
STRING threatID
```

- Los atributos representarían:

`type`: sería obligatorio e identificaría genéricamente la naturaleza de la amenaza detectada por el sistema de seguridad.



threatID: también obligatorio, recogería el identificador unívoco correspondiente a la amenaza que facilitaría el seguimiento en el árbol de ataque del avance de éste y por tanto permitiría el recálculo del riesgo.

- Clase EXPLOIT TYPE

- Se compondría del atributo:

STRING vulnerabilityID

- El atributo representaría:

vulnerabilityID: recogería el identificador unívoco correspondiente a la vulnerabilidad, si bien en caso de desconocerse podría tratarse como “unknown”.

- Clase SECURITY STATE

- Se compondría del atributo:

STRING state

- El atributo representaría:

state: sería obligatorio e identificaría la medida adoptada por el sistema que detectó el evento de seguridad, frente a éste.

La aplicación efectiva de este modelo, impondría una serie de requisitos para los sistemas involucrados en la comunicación, en particular:

- Las herramientas de seguridad deberían ser capaces, o proveer mecanismos para poder:

- Configurar el activo protegido en consonancia con los contemplados en el AARR.
  - Detectar el incidente y generar la correspondiente alerta cuando exista un nivel de certitud umbral que descarte los falsos positivos, en paralelo con las restantes funcionalidades propias de la herramienta.
  - Exportar información en el formato aquí expuesto (*IODEF-DRA*).
  - Comunicarse con la herramienta de AARR para enviarle los datos exportados en el formato (la comunicación debería producirse preferiblemente bajo condiciones adecuadas de seguridad como las identificadas).
- Por su parte, la herramienta de AARR requeriría:
- Capacidad de catalogar e identificar unívocamente los activos con códigos compatibles con los aquí referenciados.
  - Recibir comunicaciones en tiempo real (configuración modo push), o constatar de manera continua la existencia de notificaciones de algún repositorio al efecto (configuración modo pull).
  - Importar los datos conforme al modelo IODEF extendido (*IODEF-DRA*).
  - Bajo condiciones ideales de seguridad, verificar la autenticidad (en relación al sistema que generó la alerta) e integridad de los datos procesados.
  - Validar que los datos relativos a la identificación de activos son correctos y corresponden con los configurados en la herramienta. Adicionalmente, sería relevante que existiera un mapeo similar en relación al identificador de la amenaza detectada.
  - Reevaluar el riesgo bajo las nuevas condiciones de seguridad.
  - Mostrar el nuevo mapa de riesgo, considerando la fiabilidad relativa (caracterizada mediante el atributo Confidence) de la información procesada.

#### 4.4 Prueba de Concepto de Análisis de Riesgos Dinámico mediante el Modelo IODEF-DRA

Partiendo del AARR sobre un Sistema de Información sencillo, compuesto por un conjunto limitado de activos que incluyen: personal, sala de equipos en una instalación remota, equipos y datos, se generaría un Árbol de Ataque (*ver Figura 4.7*) que contemplase el nivel de riesgo asociado a la materialización de las amenazas, en el estado inicial para cada nodo. Este sería el equivalente a un AARR estático, realizado con la herramienta de AARR en base a la metodología que aplique. Para este cálculo se tendrían en consideración las diferentes circunstancias que concurren a nivel de la organización, tanto organizativas, como técnicas y humanas.

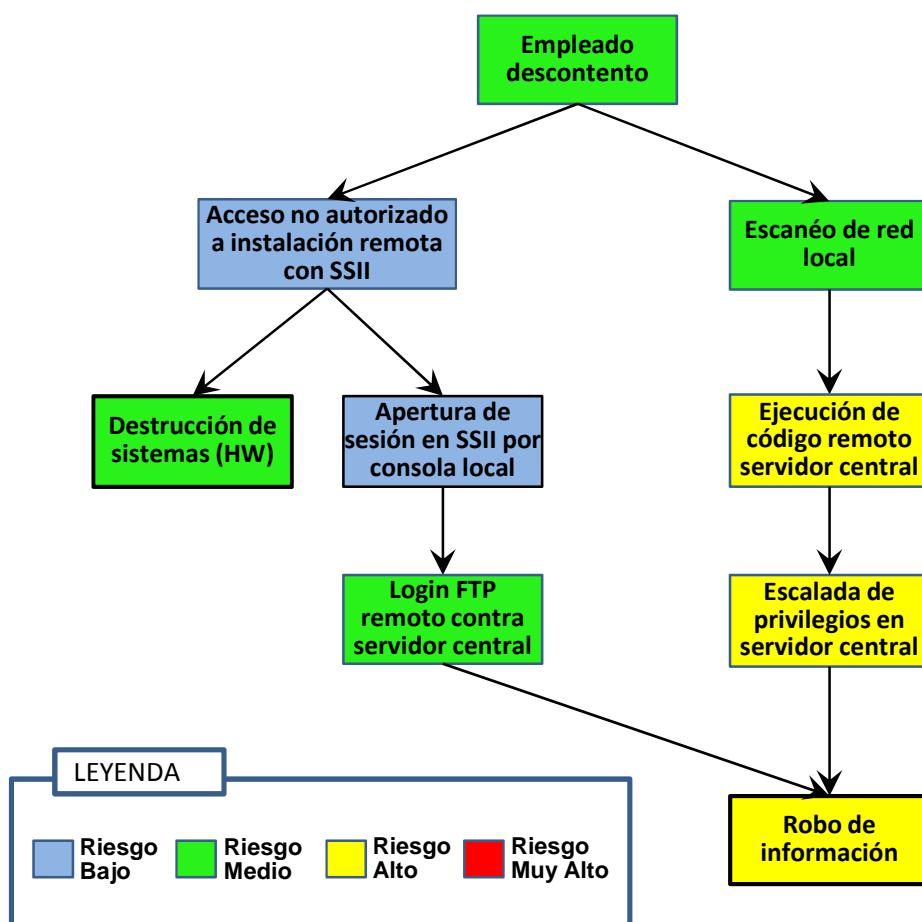


Figura 4.7 - Ejemplo de árbol de ataque para la prueba de concepto de IODEF-DRA

El proceso de AARR a desarrollar para llegar a dichos cálculos no es el foco de interés de este estudio, por lo que se simplificará. Un código de colores muestra el nivel de riesgo de partida para cada nodo como resultado del análisis de riesgos inicial. En el árbol de ataque tomado como ejemplo, un empleado disconforme con la compañía pudiendo causarle daños por dos vías. Por un lado, podría realizar un escaneo de red y lanzar un ataque contra un servidor de datos central. Por el otro podría forzar la entrada a una instalación remota y desatendida, para a continuación, bien dañar físicamente los equipos o bien utilizarlos para lanzar un ataque informático desde un segmento de red menos protegido. El objetivo más crítico (de mayor riesgo inicialmente) sería el robo de información, siendo el camino más plausible para llegar a lograrlo, la ejecución de código remoto en el servidor desde un equipo de usuario y la posterior escalada de privilegios.

Las principales ventajas que ofrecería la integración de los sistemas de seguridad con una herramienta de Análisis de Riesgos Dinámico (aplicación que implementa una metodología reconocida, y que se adhiere al formato IODEF-DRA), en el escenario propuesto, serían:

- Una herramienta de DRA basada en un enfoque metodológico adecuado podría tener el conocimiento de aquellos datos considerados críticos dentro del Sistema de Información, y de los servidores que los alojan, en tanto que un sistema de seguridad a más bajo nivel podría ser ignorante de esta información.
- El administrador de un sistema de seguridad del Sistema de Información probablemente no tendrá acceso a la información sobre la seguridad física en las instalaciones, mientras que la herramienta DRA estaría capacitada para establecer una relación con los sistemas de seguridad física en la instalación remota, permitiéndole establecer la cadena de eventos que conducen al robo de información o a la destrucción de sistemas más o menos críticos.
- La herramienta DRA tendría conocimiento de las medidas de autenticación o los procedimientos relacionados con conexiones FTP desde equipos remotos y los flujos

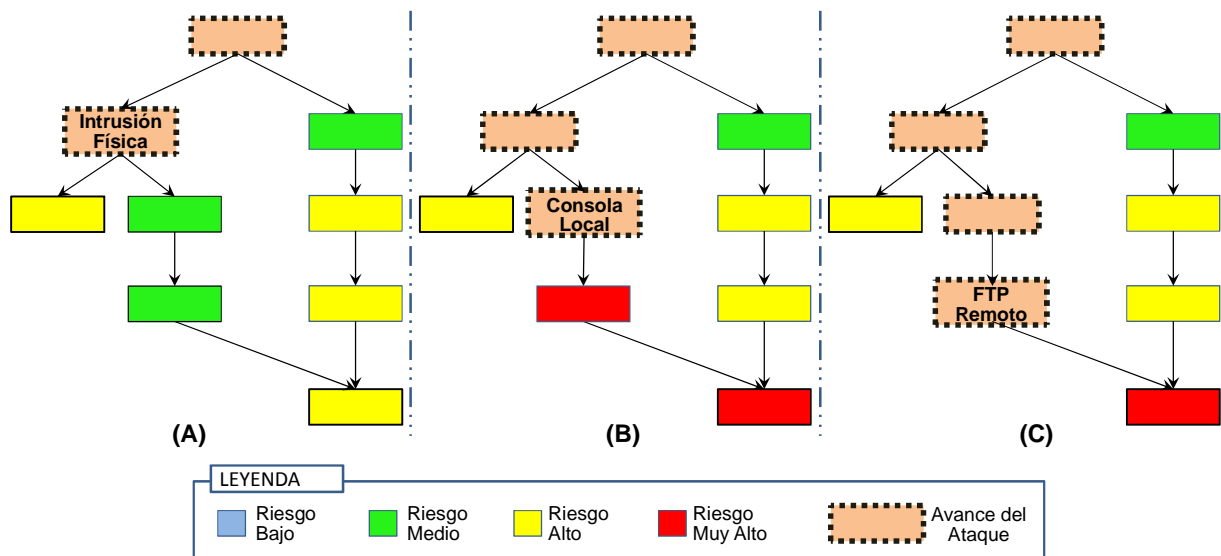
de información entre ellos, lo que sería de gran utilidad para el análisis del riesgo durante el ataque.

En base a la integración de los sistemas de seguridad, tanto lógica como física en torno al Sistema de Información (*ver Figura 4.2*), la herramienta de AARR se mantiene a la espera activa de mensajes sobre eventos de seguridad que aquellos le notifiquen. La cadena de eventos e interacciones con la herramienta DRA, que tendría lugar a lo largo del incidente de seguridad, se explica a continuación:

1. Un sistema de seguridad física detecta en primera instancia una intrusión en la sala de equipos. Al tratarse de una instalación remota la reacción por parte de un equipo de seguridad se vería obstaculizada. A través de la centralita del sistema anti-intrusión la alarma llega a la consola de monitorización de vigilancia, capaz de notificar mediante un mensaje IODEF-DRA como el ilustrado a continuación (*ver Apéndice A –Mensaje A*), a la herramienta de AARR.
2. La herramienta DRA recalcula el riesgo en tiempo real, estimándose los nuevos valores del riesgo, para los nodos susceptibles de ser afectados por la nueva situación (*ver Figura 4.8-A*).
3. A continuación, el atacante logra conectar localmente a la consola de uno de los equipos alojados en la instalación remota, tras varios intentos fallidos detectados por el HIDS (Host-based IDS) instalado. Éste reacciona, notificando a la herramienta DRA el evento de intentos fallidos de login mediante un mensaje IODEF-DRA específico (*ver Apéndice A – Mensaje B*).
4. La herramienta DRA procesa el mensaje y reevalúa el nivel de riesgo en los nodos de nuevo (*ver Figura 4.8-B*). En el contexto actual, la herramienta DRA juzga que el nodo que representa el robo de información pasa a ser fácilmente alcanzable por el atacante, al estar al tanto de que las conexiones FTP desde los servidores remotos no

son bloqueadas debido a requisitos de negocio, conforme a la política de seguridad. Por tanto, el nivel de riesgo del nodo, aumenta al nivel más elevado.

5. El siguiente paso del atacante es lanzar un login remoto vía FTP contra uno de los servidores de la organización. En este caso, un NIDS (Network IDS) monitorizando la red detectaría esta actividad que no se ajustaría a los patrones normales de comunicación de datos al servidor central, siendo capaz de notificar mediante otro mensaje IODEF-DRA (ver Apéndice A – Mensaje C) a la herramienta DRA.
6. En este caso, la certitud de que la conexión FTP sea indicativa de un evento de seguridad sería menor, al poder tratarse de un evento justificado por una excepción en la operativa del sistema. Sin embargo, la herramienta DRA estaría al tanto de la cadena de eventos previa, y afianzaría la evaluación del alto riesgo relacionado con el robo de la información (ver Figura 4.8-C).
7. El atacante habría pasado a estar conectado al servidor de datos central, pudiendo a continuación buscar la información crítica que llevarse consigo.



**Figura 4.8 - Evolución del riesgo calculado en el árbol de ataque mediante DRA**

El cálculo del riesgo en tiempo real, refleja a lo largo del ataque el aumento del riesgo en el nodo final, que representa la captura de la información sensible. De este modo la visión de conjunto proporcionada por una metodología de AARR unida a la actualización del nivel de riesgo conforme al avance del atacante podría haber permitido frustrar mediante una intervención preventiva, el hecho de que el usuario alcanzara la información sensible a proteger.

Si nadie estableciera la relación entre los diferentes eventos acaecidos, la información crítica podría ser sustraída a través de la conexión FTP antes de que el personal de seguridad se personara en la instalación remota en respuesta a la alarma del sistema de seguridad física. Por el contrario, monitorizar el riesgo mediante la herramienta DRA ayudaría a la toma de decisiones, como el cierre de las conexiones FTP remotas desde el sistema en la instalación remota afectado por el ataque. El negocio podría resultar parcialmente afectado, si bien la evaluación por parte de la herramienta reflejaría que el robo de información sería aún más grave.

## 5 CONCLUSIONES Y TRABAJO FUTURO

---

Son múltiples las soluciones que han contemplado en alguna medida los retos que plantea el AARR Dinámico, cubriendo algunos de los aspectos fundamentales. El desarrollo de métodos y tecnologías que abordan problemáticas particulares, dentro del conjunto de variables que influyen en la evaluación del riesgo, permite encarar desde diferentes ángulos esta tarea.

Esta multiplicidad de planteamientos no facilita un enfoque cooperativo e integrador, que aporte una visión más completa. Por el contrario, las soluciones tienden a centrarse en un ámbito que con mayor o menor eficacia puede contemplar los cambios surgidos en dicho ámbito (nuevas vulnerabilidades, detección de ataques, etc.) pero no alcanzan una visión de conjunto, que abarque los múltiples cambios que podrían afectar al riesgo.

A través del modelo de datos extendido IODEF-DRA aquí presentado se pretende englobar la visión de conjunto a través de herramientas de AARR, basadas en metodologías reconocidas que puedan recibir información de múltiples fuentes sobre eventos de seguridad en un formato que les permita su integración y análisis en tiempo real. La aplicación efectiva de estas comunicaciones, basada en un esquema de datos como el propuesto, entre los sistemas de seguridad de la Organización, u otras fuentes externas de confianza tales como CERTs, y las herramientas de AARR, repercutiría en los siguientes beneficios:

- Capacidad para actualizar los procesos de AARR en tiempo real, ofreciendo la posibilidad de una monitorización continuada de su evolución, que permita una percepción instantánea del riesgo sobre los objetivos del negocio, así como una respuesta más rápida.
- Aplicación de un enfoque metodológico del AARR, de utilidad tanto a nivel técnico como a alto nivel. Este enfoque conduciría a una visión homogénea del riesgo en la Organización, que aportaría una respuesta ante los incidentes mejor alineada con las políticas de seguridad.



- Posibilidad de tener en consideración activos de nivel superior de la Organización, tales como componentes de seguridad, políticas u otros factores organizativos más allá de la mera arquitectura del Sistema de Información. La integración de los sistemas de seguridad con el AARR Dinámico y metodológico expandiría el dominio evaluado al propio Sistema de Información y su entorno.

El escenario recogido en la prueba de concepto muestra cómo la integración propuesta mediante el uso de IODEF-DRA, evidencia las mencionadas ventajas. En primer lugar permitió monitorizar y detectar el aumento del riesgo, teniendo en cuenta el impacto de los activos en los objetivos del negocio. Proporcionó una visión unificada del riesgo, tanto desde el punto de vista técnico como del de gestión, facilitando la toma de decisiones. Finalmente, integró la seguridad física en torno al Sistema de Información, y tuvo en cuenta aspectos relacionados con las políticas de seguridad para evaluar el riesgo en tiempo real.

## **5.1 Trabajo Futuro**

El planteamiento de trabajo futuro se orienta a la evolución del proceso de captura de datos, orientados al AARR Dinámico, que permitiría mejorar la calidad y fiabilidad de los AARR. Para ello, se seguirán las siguientes líneas de acción principalmente:

1. Desarrollo y promoción del uso del modelo IODEF-DRA, a través de su adopción mediante herramientas de seguridad.
2. Evolución de herramientas de AARR, basadas en metodologías reconocidas, orientadas a la integración de capacidad para desarrollo de AARR dinámicos (DRA).
3. Finalmente, adopción de otras fuentes de información que diversifiquen el input que reciben las herramientas DRA, para obtener una base de conocimiento en tiempo real más completa que optimice la evaluación del riesgo.

## 5.2 Divulgación de Resultados

En paralelo al desarrollo de este proyecto, se han elaborado dos artículos condensando sus contenidos y recogiendo los resultados alcanzados, ambos aceptados para su presentación como comunicación oral, en la XII Reunión Española sobre Criptología y Seguridad de la Información (RECSI 2012) y bajo los siguientes títulos:

- D. López, O. Pastor, and L.J. García Villalba, “**Concepto y Enfoques sobre el Análisis y la Gestión Dinámica del Riesgo en Sistemas de Información**”.
- D. López, O. Pastor, and L.J. García Villalba, “**Comunicación de Eventos de Seguridad orientada al Análisis de Riesgos Dinámico**”.

Adicionalmente, se ha procedido al envío de un artículo de mayor extensión a la revista sectorial e internacional **Risk Analysis**, que se encuentra actualmente en proceso de revisión y a la espera de aceptación.

## REFERENCIAS

---

- [1] *Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.*
- [2] *Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.*
- [3] *Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.*
- [4] *Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.*
- [5] Series CCN-STIC: “Normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las tecnologías de la información y las comunicaciones de la Administración”, [Online]. Available:  
[https://www.ccn.cni.es/index.php?option=com\\_content&view=article&id=6&Itemid=9](https://www.ccn.cni.es/index.php?option=com_content&view=article&id=6&Itemid=9)
- [6] ISO/IEC 31000:2009, *Risk management - Principles and guidelines*, International Organization for Standardization, 2009.
- [7] ISO/IEC 27005:2008, *Information technology - Security techniques - Information security risk management*, International Organization for Standardization, 2008.
- [8] UNE 71504:2008, *Tecnología de la Información (TI) - Metodología de análisis y gestión de riesgos para los sistemas de información*, AENOR, 2008.
- [9] MAGERIT versión 2, *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. I Método*, Ministerio de Administraciones Públicas (MAP), España, 2006.
- [10] C. Alberts, and A. Dorofee “Managing Information Security Risk. The OCTAVE Approach”, in *Addison Wesley*, 2005.
- [11] Siemens - Insight Consulting, *The Logic behind CRAMM’s Assessment of Measures of Risk and Determination of Appropriate Countermeasures*, Siemens, 2005.
- [12] 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.
- [13] BSI IT *Baseline Protection Manual Bundesamt für Sicherheit in der Informationstechnik*, Federal Office for Information Security (BSI), Deutschland, 2000.

- [14] G. Stoneburner, A. Goguen, and A. Feringa, “Risk Management Guide for Information Technology Systems”, in *NIST Special Publication 800-30*, 2002.
- [15] 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
- [16] ISO/IEC 27001:2005, *Information technology - Security techniques - Information security management systems - Requirements*, International Organization for Standardization, 2005.
- [17] 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.
- [18] 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*, TECNIMAP-Iniciativa 80, 2010.
- [19] 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.
- [20] K. Voss, Ch. Carlsson, and A. Akademi, “Consultant Service and Dynamic Risk Assessment”, in *IST-AssessGrid project WP.3*, Sixth Framework Programme, 2008.
- [21] 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.
- [22] W. Qi, X. Liu, J. Zhang, and W. Yuan, “Dynamic Assessment and VaRBased Quantification of Information Security Risk”, in *2nd International e-Business and Information System Security Conference (EBISS)*, pp.1-4, 22-23, 2010.
- [23] 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.
- [24] 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.
- [25] 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.

- [26] 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*, U. S. Patent no: US 6219805 B1, 2001.
- [27] National Institute of Standards and Technology (NIST) "National Vulnerability Database", [Online]. Available: <http://nvd.nist.gov>
- [28] 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.
- [29] 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.
- [30] 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.
- [31] 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.
- [32] 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.
- [33] 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, 23-24, May. 2007.
- [34] 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.
- [35] 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.
- [36] M. Nicolett, and K.M. Kavanagh, "Magic Quadrant for Security Information and Event Management (SIEM)", in *Gartner*, Research Report, no.G00176034, May. 2010.
- [37] A. Årnes, 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.
- [38] 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.
  - [39] 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.
  - [40] 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.
  - [41] 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.
  - [42] 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.
  - [43] W. Kanoun, N. Cuppens-Boulahia, F. Cuppens, and F. Autrel, "Advanced Reaction Using Risk Assessment in Intrusion Detection Systems", in *2nd International Workshop on Critical Information Infrastructures Security (CRITIS'07)*, pp.58-70, Oct. 2007.
  - [44] ISO/IEC 27035:2011, *Information technology - Security techniques - Information security incident management*, International Organization for Standardization, 2011.
  - [45] H. Debar, D. Curry, and B. Feinstein, "Intrusion Detection Message Exchange Format (IDMEF)", Internet Engineering Task Force (IETF), RFC-4765, Mar. 2007. [Online]. Available: <http://datatracker.ietf.org/doc/rfc4765>
  - [46] R. Danyliw, J. Meijer, and Y. Demchenko, "Incident Object Description and Exchange Format (IODEF)", Internet Engineering Task Force (IETF), RFC-5070, Dec. 2007. [Online]. Available: <http://datatracker.ietf.org/doc/rfc5070>
  - [47] P. Kothari, *Intrusion Detection Interoperability Standardization*, SANS Institute - InfoSec Reading Room, Feb. 2002.
  - [48] K. Gorzelak, T. Grudziecki, P. Jacewicz, P. Jaroszewski, L. Juszczuk, and P. Kijewski, *Proactive Detection of Network Security Incidents*, European Network and Information Security Agency (ENISA), Report Deliverable 2011-12-07, pp.114-116, 2011.

- [49] Standardisation Activities, European Network and Information Security Agency (ENISA), [Online]. Available: <http://www.enisa.europa.eu/act/cert/background/inv/cert-activities/standardisation/standard-ii>
- [50] Y. Demchenko, "IODEF Design principles and IODEF Data Model Overview", in *5th TF-CSIRT: IODEF WG*, 2002. [Online]. Available: <http://www.terena.org/activities/tf-csirt/meeting5/demchenko-iodef-design-datamodel.pdf>
- [51] Y. Demchenko, "Incident Object Description and Exchange Format Requirements", TERENA - IODEF Network Working Group, Oct. 2002. [Online]. Available: <http://tools.ietf.org/html/draft-ietf-inch-iodef-rfc3067bis-requirements-00>
- [52] Incident Object Data Model v.0.05 Final, TERENA - IODEF Working Group, Feb. 2002. [Online]. Available: <http://www.terena.nl/tech/task-forces/tf-csirt/iodef/docs/iodef-datamodel-draft-003.html>
- [53] S. Tesink, "Improving CSIRT Communication Through Standardized and Secured Information Exchange", in Master thesis, Tilburg University, Dec. 2005.
- [54] P. Cain, and D. Jevans, "Extensions to the IODEF-Documents Class for Reporting Phishing", Internet Engineering Task Force (IETF), RFC-5901, Jul. 2010. [Online]. Available: <http://datatracker.ietf.org/doc/rfc5901>
- [55] K. Moriarty, "Real-time Inter-network Defense (RID) ", Internet Engineering Task Force (IETF), RFC-6045, Nov. 2010. [Online]. Available: <http://datatracker.ietf.org/doc/rfc6045>

## APÉNDICE A - EJEMPLO DE MENSAJES IODEF-DRA PARA PRUEBA DE CONCEPTO (XML)

---

### *Mensaje A*

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- This example shows a remote premise physical break-in
detected by a security system and notified using IODEF-DRA -->
<IODEF-Document version="1.00" ="1.00" lang="en"
xmlns="urn:ietf:params:xml:ns:iodef-1.0"
xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance
xsi:schemaLocation="urn:ietf:params:xml:schema:iodef-1.0">
  <Incident purpose="reporting">
    <IncidentID name="physicalAlert">000001</IncidentID>
    <ReportTime>2012-03-10T20:13:05+00:00</ReportTime>
    <Assessment>
      <Impact severity="medium" completion="succeeded"/>
      <Confidence rating="high"/>
    </Assessment>
    <Contact role="admin" type="person">
      <Description>Security Staff on site</Description>
    </Contact>
    <EventData>
      <DetectTime>2012-03-10T20:13:02+00:00</DetectTime>
      <Assessment>
        <Impact severity="medium" completion="succeeded"/>
        <Confidence rating="high"/>
      </Assessment>
      <AdditionalData>
        <AffectedAsset type="site" assetID="remote-site"/>
        <ReportingSystem type="physicalSecurityConsole"
systemID="console01"/>
        <DetectedThreat type="unauthorized access"
threatID="Breakin"/>
        <ExploitType vulnerabilityID="unknown"/>
        <SecurityState state="supervised"/>
      </AdditionalData>
    </EventData>
  </Incident>
</IODEF-Document>
```



## ***Mensaje B***

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- This example shows a local console login, after several
failed login attempts, detected by a security system and notified
using IODEF-DRA -->
<IODEF-Document version="1.00" = "1.00" lang="en"
xmlns="urn:ietf:params:xml:ns:iodef-1.0"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="urn:ietf:params:xml:schema:iodef-1.0">
  <Incident purpose="reporting">
    <IncidentID name="HostIDSAAlert">000015</IncidentID>
    <ReportTime>2012-03-10T20:18:33+00:00</ReportTime>
    <Assessment>
      <Impact severity="low" completion="succeeded"/>
      <Confidence rating="high"/>
    </Assessment>
    <Contact role="admin" type="person">
      <Description>Network administrator</Description>
    </Contact>
    <EventData>
      <DetectTime>2012-03-10T20:18:25+00:00</DetectTime>
      <Assessment>
        <Impact severity="low" completion="succeeded"/>
        <Confidence rating="high"/>
      </Assessment>
      <AdditionalData>
        <AffectedAsset type="host" assetID="Remoteserver"/>
        <ReportingSystem type="HIDS" systemID="HIDS08"/>
        <DetectedThreat type="Local console login failure"
threatID="FailedLoginAttempts"/>
        <ExploitType vulnerabilityID="unknown"/>
        <SecurityState state="supervised"/>
      </AdditionalData>
    </EventData>
  </Incident>
</IODEF-Document>
```

## *Mensaje C*

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- This example shows a remote FTP login against the central
data server violating communication policies, detected by a
security system and notified using IODEF-DRA -->
<IODEF-Document version="1.00" = "1.00" lang="en"
xmlns="urn:ietf:params:xml:ns:iodef-1.0"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="urn:ietf:params:xml:schema:iodef-1.0">
  <Incident purpose="reporting">
    <IncidentID name="NetworkIDSAlert">000059</IncidentID>
    <ReportTime>2012-03-10T20:21:18+00:00</ReportTime>
    <Assessment>
      <Impact severity="low" completion="succeeded"/>
      <Confidence rating="medium"/>
    </Assessment>
    <Contact role="admin" type="person">
      <Description>Network administrator</Description>
    </Contact>
    <EventData>
      <DetectTime>2012-03-10T20:21:13+00:00</DetectTime>
      <Assessment>
        <Impact severity="low" completion="succeeded"/>
        <Confidence rating="medium"/>
      </Assessment>
      <AdditionalData>
        <AffectedAsset type="host" assetID="Fileserver"/>
        <ReportingSystem type="NIDS" systemID="NIDS01"/>
        <DetectedThreat type="Remote FTP connexion"
threatID="RemoteFTP"/>
        <ExploitType vulnerabilityID="unknown"/>
        <SecurityState state="supervised"/>
      </AdditionalData>
    </EventData>
  </Incident>
</IODEF-Document>
```