III. OTRAS DISPOSICIONES

MINISTERIO DE DEFENSA

163 *Resolución 420/38203/2015, de 22 de diciembre, de la Secretaría General Técnica, por la que se publica el Convenio de colaboración con la Universidad Politécnica de Madrid para el desarrollo de una herramienta de visualización y trazado en un ciberataque.*

Suscrito el 3 de diciembre de 2015 el Convenio de colaboración entre el Ministerio de Defensa y la Universidad Politécnica de Madrid para el desarrollo de una herramienta de visualización y trazado en un ciberataque, en cumplimiento de lo dispuesto en el artículo 8.2 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, procede la publicación en el «Boletín Oficial del Estado» de dicho convenio, que figura como anexo de esta resolución.

Madrid, 22 de diciembre de 2015.–El Secretario General Técnico del Ministerio de Defensa, David Javier Santos Sánchez.

ANEXO

Convenio específico entre el Ministerio de Defensa y la Universidad Politécnica de Madrid para el desarrollo de una herramienta de visualización y trazado de un ciberataque

En Madrid a 3 de diciembre de 2015.

REUNIDOS:

De una parte: El Excmo. Almirante General D. Fernando García Sánchez, Jefe de Estado Mayor de la Defensa, en uso de las facultades que le fueron delegadas por el titular del Ministerio de Defensa de acuerdo con la Orden DEF/3015/2004, de 17 de septiembre, sobre delegación de competencias en autoridades del Ministerio de Defensa en materia de convenios de colaboración.

De otra parte: D. Roberto Prieto López, Vicerrector de Investigación de la Universidad Politécnica de Madrid (CIF Q-2818015F), en adelante, UPM, en nombre y representación de la misma, en virtud de la delegación de competencias otorgada por el Excmo. y Magfco. Sr. Rector de la UPM, con fecha 2 de enero de 2013.

Las partes, reconociéndose capacidad jurídica, competencia y legitimación suficientes para obligarse y a tal efecto suscribir el presente Convenio Específico,

EXPONEN:

Primero.

Este convenio se firma al amparo del Acuerdo Marco de colaboración entre el Ministerio de Defensa y la Universidad Politécnica de Madrid, para la formación, investigación y desarrollo de actuaciones en materia de ciberdefensa, suscrito el 6 de noviembre de 2013, en adelante, el Acuerdo Marco.

Segundo.

El citado Acuerdo Marco tiene por objeto establecer la cooperación entre el Ministerio de Defensa (MINISDEF) y la Universidad Politécnica de Madrid (UPM), dentro del ámbito de sus respectivas competencias, dirigida a la formación de personal cualificado en

cve: BOE-A-2016-163
Verificable en http://www.boe.es

Ciberdefensa, así como para el desarrollo de estudios, investigaciones y actuaciones conjuntas en ese ámbito. Para hacer efectiva la realización de éste objeto, las partes firmantes establecerán mediante convenios específicos los proyectos concretos con el fin de realizar diferentes actuaciones, entre las que se encuentra «realizar estudios y proyectos de investigación y desarrollo en esta materia» (Ciberdefensa)

Tercero.

El Ministerio de Defensa, representado por el Mando Conjunto de Ciberdefensa (MCCD) está interesado en la colaboración del Departamento de Ingeniería de Sistemas Telemáticos adscrito a la Escuela Técnica Superior de Ingenieros de Telecomunicación de la UPM, para desarrollar un programa de colaboración en investigación y fomento de la formación del personal, a través de la ejecución de diversos trabajos de carácter técnico, centrados en el desarrollo de una herramienta de visualización y trazado de un ciberataque.

Por todo ello las partes formalizan el presente convenio específico, que se regirá por las siguientes

CLÁUSULAS:

Primera. *Objeto.*

Este convenio específico de colaboración tiene por objeto la realización de las actuaciones concretas en desarrollo del objeto del Acuerdo Marco de Colaboración entre el Ministerio de Defensa (MINISDEF) y la Universidad Politécnica de Madrid (UPM) para la formación, investigación y desarrollo de actuaciones en materia de ciberdefensa, en lo concerniente a la realización de actividades centradas en el fomento de la investigación y la formación técnica, concretadas en el estudio y desarrollo de una herramienta de visualización y trazado de un ciberataque, según los objetivos y plan de trabajo definidos en el anexo a este documento.

Segunda. *Aportaciones de la UPM.*

La UPM se compromete a:

a) Mantener la adecuada dotación económica y de medios de los grupos de trabajo necesarios para sus fines.

b) Designar a un profesor director de los trabajos y a que se realicen los trabajos que se describen en el anexo de este convenio en la forma y condiciones pactadas en el mismo, responsabilizándose de que hayan sido concedidas las autorizaciones reguladas en la normativa vigente y de la ordenación y aplicación de gastos y pagos relativos al objeto del convenio.

c) Designar al personal por su capacidad técnica y, en función del grado de clasificación de la información manejada, considere oportuno que intervenga en la realización de las tareas específicas derivadas de la ejecución de este convenio, de manera que el proyecto contribuya a la mejora de la formación técnica en aspectos de ciberdefensa del personal de la UPM, y a que el resto del profesorado participante lleve a cabo las obligaciones de este convenio, ejecutándolo en los términos que determine el Director de los trabajos o persona en quien delegue, y las autoridades universitarias.

d) Informar al Mando Conjunto de Ciberdefensa (MCCD), a través del director de los trabajos, acerca de la marcha de los mismos con la periodicidad establecida en el anexo.

e) Asesorar al MCCD durante las fases de implantación y explotación de la herramienta desarrollada como consecuencia del proyecto.

cve: BOE-A-2016-163
Verificable en http://www.boe.es

Tercera. *Aportaciones del MCCD.*

El MCCD se compromete a:

a) Definir los requisitos necesarios para el proyecto de colaboración.
b) Designar personal para el seguimiento y control del citado proyecto.
c) Designación de personal experto para colaboración con el personal de la UPM para el trabajo conjunto y la aclaración de las cuestiones técnicas cuando sea necesario.
d) Participar con la cantidad máxima de ciento sesenta y nueve mil quinientos diez euros con treinta y un céntimos (169.510,31 euros) para la realización de las actividades objeto del presente convenio.

Este gasto será imputado a la aplicación presupuestaria 14.02.122AN.650 del MINISDEF.
La aportación económica se efectuará mediante tres ingresos de acuerdo al siguiente calendario:

Un 40 % (67.804,13 euros) a la firma del convenio.
Un 30 % (50.853,09 euros) asociado al cumplimiento del hito 3 definido en el anexo.
Un 30 % (50.853,09 euros) a la terminación satisfactoria de la totalidad de las tareas descritas en el anexo.

El abono de dichas cantidades se hará efectivo mediante transferencia bancaria a la cuenta n.º 0065 0100 12 0031000262, del Barclays Bank, plaza de Colón, 2, 28046 Madrid, a nombre de Universidad Politécnica de Madrid-Investigación Transferencia Tecnológica.
La Oficina de Transferencia de Tecnología (OTT) será la unidad administrativa de la UPM encargada de la gestión y administración del convenio, en cuanto a su registro, cobros, pagos, obligaciones fiscales y demás servicios de apoyo de carácter administrativo derivados de la realización del mismo.

Cuarta. *Titularidad de los resultados del proyecto de desarrollo.*

Corresponde a MINISDEF la titularidad de los resultados del proyecto de desarrollo objeto de este convenio.
La UPM podrá utilizar la formación técnica adquirida en el desarrollo del proyecto; siempre con el cumplimiento estricto de la cláusula de confidencialidad de la información estipulada en el Acuerdo Marco.

Quinta. *Medidas de control y seguimiento.*

El control y seguimiento se llevará a cabo por la Comisión de Seguimiento del Acuerdo Marco.

Sexta. *Confidencialidad.*

Los aspectos relacionados con la confidencialidad se regirán por las disposiciones al efecto estipuladas en el Acuerdo Marco.
La Comisión de Seguimiento del Acuerdo Marco determinará en cada momento, en función del grado de clasificación de la información manejada y otros criterios, el lugar de realización de los trabajos.

Séptima. *Vigencia.*

El presente convenio tendrá una duración de doce meses a partir de la fecha de su firma.

cve: BOE-A-2016-163
Verificable en http://www.boe.es

Octava. *Causas de resolución.*

Este convenio podrá resolverse por mutuo acuerdo entre las partes, bien porque consideren finalizado el desarrollo del proyecto,antes del período marcado, o por cualquier otra causa que haga inviable, inconveniente o no rentable su prosecución.

El incumplimiento grave de cualquiera de las obligaciones contraídas por el presente convenio por una de las partes, facultará a la otra para resolver el mismo, quedando automáticamente anulados todos los derechos y obligaciones correspondientes sobre el objeto del convenio.

La comunicación a la otra parte de la decisión de resolución del convenio deberá realizarse mediante denuncia expresa con seis meses de antelación a la finalización de su vigencia, notificándose tal intención con un preaviso de un mes.

Las disposiciones del apartado «Confidencialidad» subsistirán después de la terminación o resolución del convenio.

Novena. *Legislación aplicable.*

Al presente convenio, de naturaleza administrativa, no le es de aplicación el Texto Refundido de la Ley de Contratos del Sector Público, aprobado por el Real Decreto Legislativo 3/2011, de 14 de noviembre, en virtud de la exclusión contenida en el artículo 4.1 c) del citado texto legal, salvo que, en ejecución de este convenio, hubieran de suscribirse contratos que, por su naturaleza, tengan la consideración de contratos sujetos al citado texto refundido.

En materia presupuestaria, económica y financiera se atendrá al contenido de la Ley 47/2003, de 26 de noviembre, General Presupuestaria.

Las controversias surgidas entre las partes se resolverán de mutuo acuerdo en el seno de la comisión de seguimiento prevista en la cláusula quinta, acudiendo, en lo posible, a los principios establecidos en el indicado Texto Refundido de la Ley de Contratos del Sector Público y en el resto del ordenamiento jurídico administrativo.

A este convenio le son de aplicación las normas contenidas en el título III, capitulo III, de los Estatutos de la UPM y en la normativa para la realización de trabajos de carácter científico, técnico o artístico, así como para el desarrollo de enseñanzas de especialización o actividades específicas de formación (aprobada en Junta de Gobierno de 27 de febrero de 2003) que regulan las condiciones y procedimientos de autorización que se aplican en la UPM.

Las cuestiones litigiosas que puedan surgir en la interpretación de este convenio y que no hayan sido resueltas por la comisión de seguimiento, se someterán al orden jurisdiccional contencioso-administrativo.

Habiendo leído el presente por sí mismos y hallándose conformes, lo firman por duplicado y a un solo efecto, en lugar y fecha anteriormente citados.–Por el Ministerio de Defensa, el Jefe de Estado Mayor de la Defensa, Fernando García Sánchez.–Por la Universidad Politécnica de Madrid, el Vicerrector de Investigación, Roberto Prieto López.

ANEXO

Herramienta de visualización y trazado de un ciberataque

1. Objeto.

En este documento se describe la línea de I+D sobre «Herramienta de visualización y trazado de un ciberataque» a desarrollar en este convenio MCCD-UPM, conforme a lo planteado en [1].

2. Introducción.

El concepto de «Visual Analytics» se refiere a la ciencia de razonamiento analítico soportado por interfaces visuales interactivos. Hoy en día, se producen datos a una

cve: BOE-A-2016-163
Verificable en http://www.boe.es

velocidad increíble, y en muchos casos la naturaleza compleja de problemas hace imprescindible la inclusión de inteligencia humana para los procesos de análisis de datos. Los métodos de «Visual Analytics» permiten a las personas combinar la flexibilidad, creación y conocimiento humano con las capacidades de almacenamiento y procesado proporcionados por los ordenadores. De esta forma, las personas pueden interactuar directamente con las capacidades de análisis de los ordenadores, utilizando interfaces visuales avanzadas, permitiendo tomar decisiones con información suficiente en situaciones complejas [2].

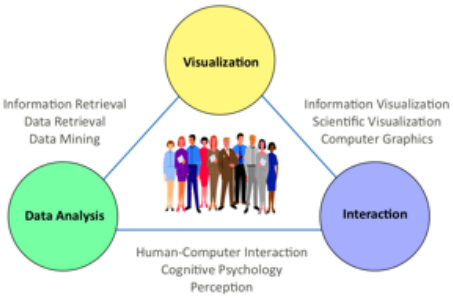

Figura 1: Visual Analytics

Figura 1: Visual Analytics

El área de la Seguridad en Redes y Sistemas, y más concretamente, los aspectos de Detección de Intrusiones es uno de los campos más atractivos para la aplicación de los métodos de Visual Analytics, de forma que es posible representar visualmente aquellos parámetros que se consideren convenientes de una forma visual para que un administrador de seguridad de un dominio pueda tener de una forma sencilla y fácil distintas visiones gráficas (desde las más detalladas a las más generales) del estado de seguridad de las redes, servicios y sistemas en su dominio.

3. Objetivos.

De acuerdo con lo establecido en [1], la presente línea de trabajo se centra en el desarrollo de una herramienta que permita visualizar y trazar un ciberataque así como determinar probabilísticamente su evolución, de forma que se permita el apoyo a la toma de decisiones. La herramienta debería mostrar:

Nivel de compromiso: en base a los dispositivos vulnerados por un atacante (camino seguido) y/o en base a indicadores de compromiso reconocidos o a desarrollar.
Características del compromiso: Cada ataque tiene una serie de características que lo diferencia del resto (tipo de vulnerabilidades explotadas, tiempos empleados, velocidad, magnitud, virulencia, persistencia, etc.).
Técnicas utilizadas: tanto las de éxito como las que no (pruebas, intentos).
Origen potencial del ataque.

Además, debe incluir interfaces de navegación basadas en estratificación por capas para que la información se muestre para su empleo por personal estratégico, operacional y táctico. De esta manera, se pueda ir de la información más general (nivel estratégico) al dato más detallado (nivel táctico).
Con objeto de facilitar la obtención temprana de resultados, se considerará la existencia de software de código libre que pueda ser reutilizado en las herramientas a desarrollar. Así mismo, el software desarrollado servirá como modelo, sobre el que se realizarán las pruebas pertinentes y extraerán lecciones aprendidas

cve: BOE-A-2016-163
Verificable en http://www.boe.es

4. Plan de trabajo.

En este apartado se detallan y planifican las tareas a realizar por UPM en esta línea de trabajo.

4.1 Tarea 1.–Análisis del Estado del Arte en Herramientas de Visualización aplicadas a la Seguridad.

En esta tarea se realizará una prospección tecnológica sobre las propuestas, desarrollos y soluciones existentes en el área general de Visual Analytics y, específicamente, en su aplicación a la visualización de incidentes de seguridad y ciberataques recibidos en Redes y Sistemas de comunicaciones propios.

Asimismo, se realizará una valoración crítica de su aplicabilidad a distintos escenarios relacionados con el contexto de la propuesta, de los que el MCCD podrá valorar su relevancia para sus propósitos. Como consecuencia de este análisis y valoración, se enumerarán las propuestas identificadas que se consideren adecuadas para un potencial uso en fases posteriores en cuanto a:

Parámetros y fuentes de datos a visualizar.
Interfaces de navegación eficaces basadas en estándares existentes.
Escenarios de visualización.

4.2 Tarea 2.–Definición de los Parámetros y Niveles de Visualización.

En esta tarea, se definirán los parámetros y fuentes de datos a visualizar, así como la distribución de parámetros de visualización en distintas categorías, de forma que se dé cumplimiento a los requisitos de definición y desarrollo de interfaces de navegación basadas en estratificación por capas para que la información se muestre para su empleo por personal estratégico, operacional y táctico. Estos requisitos vendrán definidos por la primera tarea, pero deberán ser aprobados por el MCCD, partiendo de los propuestos en la tarea 1 sin tener que circunscribirse exclusivamente a éstos (el MCCD tendrá la posibilidad de añadir y/o modificar).

4.3 Tarea 3.–Definición de los Escenarios de Visualización.

En esta tarea, se definirán los diferentes casos de uso que serán demostrados por la herramienta de visualización. En esta tarea, será necesario definir un conjunto de actividades, legítimas o ilegítimas, que podrán dar lugar a eventos de visualización en el modelo. Igualmente, se definirán los modelos de visualización correspondientes a las actividades seleccionadas.

Al menos existirán los escenarios suficientes que, en base a un hecho o conjunto de hechos, permitan representar visualmente las amenazas internas y externas ampliamente reconocidas: DoS, DDoS, fuga de información, ataques a nivel aplicación, explotación de vulnerabilidades, intrusiones, etc., en base a correlación de logs, comportamientos anómalos, etc.

4.4 Tarea 4.–Desarrollo de un modelo de Visualización.

De acuerdo a la valoración de algoritmos y herramientas realizadas en la tarea 1, se desarrollará un modelo de sistema de visualización que permita la visualización gráfica de los distintos elementos definidos en la tarea 2, y con la granularidad y clasificación necesaria según los requisitos de dicha tarea.

4.5 Tarea 5.–Desarrollo de batería de pruebas.

De acuerdo a los escenarios de visualización definidos en la tarea 3, se desarrollará un simulador de actividades, basado en una batería de pruebas que deberá aprobar el MCCD, que permita alimentar el modelo de visualización de una forma simple y modular, para que pueda ser ampliado o modificado fácilmente con otro tipo de actividades.

cve: BOE-A-2016-163
Verificable en http://www.boe.es

4.6 Tarea 6.–Integración de modelo y realización de pruebas.

En esta tarea se procederá a la integración de los diversos módulos software desarrollados en las distintas tareas para la obtención de un modelo.

Una vez obtenido el modelo, se llevarán a cabo las pruebas funcionales de las herramientas desarrolladas, así como demostraciones básicas de ejercicios de visualización de acuerdo a los escenarios definidos.

4.7 Tarea 7.–Entrega y presentación del modelo y documentación asociada.

Entrega al MCCD del modelo. El formato de entrega y presentación permitirá la ejecución del modelo en una plataforma virtualizada (en VMware (ESX)).

Además estará acompañada de una documentación que permita comprender el modelo, el contexto desarrollado y las conclusiones extraídas. Para ello se entregaran los siguientes documentos:

- Descripción técnica del modelo y sus funcionalidades.
- Resultados de las pruebas.
- Documentación de los componentes o módulos que componen el modelo, su configuración y/o los desarrollos realizados.
- Informe de conclusiones y próximos pasos (evolución del modelo).

La tabla 1 refleja la planificación temporal de las tareas definidas en el anterior apartado. Los hitos y entregas correspondientes a dichas tareas se detallan en la tabla 2.

Tabla 1.- *Plan de trabajo (meses)*

	1	2	3	4	5	6	7	8	9	10	11	12
T1. Análisis del Estado del Arte.												
T2. Definición de Parámetros y Niveles.												
T3. Definición de los Escenarios de Visualización												
T4. Desarrollo de un Prototipo de Visualización												
T5. Desarrollo de batería de pruebas												
T6. Integración y pruebas												
T7. Entrega y presentación del prototipo												

5. Hitos y entregas.

Teniendo en cuenta el plan de trabajo detallado en el epígrafe anterior, en la tabla 2 se refleja la planificación de hitos y entregas del proyecto.

Tabla 2.- Hitos y entregas

Hito	Descripción	Fecha	Entrega
H1	Análisis del Estado del Arte en Herramientas de Visualización aplicadas a la Seguridad.	Mes 3.	Documento de prospección tecnológica de la tarea 1.
H2	Definición de Requisitos.	Mes 4.	Documento con los requisitos de parámetros y escenarios de las tareas 2 y 3.
H3	Modelo básico y primeros tests de funcionalidad.	Mes 7.	Modelo y primeros tests: Corrección temprana de desviaciones del objetivo y requisitos (H2)

cve: BOE-A-2016-163
Verificable en http://www.boe.es

Hito	Descripción	Fecha	Entrega
H4	Desarrollo e integración de modelo final.	Mes 10.	Software con la implementación del modelo y batería de pruebas desarrollado en tareas 4 y 5.
H5	Batería de pruebas formal.	Mes 11.	Ejecución de la batería de pruebas.
H6	Entrega modelo final y documentación asociada.	Mes 12.	Entrega de software y documentos relativos a la tarea 7

6. Referencias.

[1] Acuerdo de colaboración MCCD-UPM. «Línea de trabajo sobre Herramienta de visualización y trazado de un ciberataque». Junio 2013.

[2] Thomas, J., Cook, K.: «Illuminating the Path: Research and Development Agenda for Visual Analytics». IEEE-Press, 2005.

cve: BOE-A-2016-163
Verificable en http://www.boe.es