

# SOLICITUD DE PARTICIPACIÓN EN LA CONVOCATORIA DE LA CÁTEDRA ISDEFE EN DEFENSA Y SEGURIDAD AL MEJOR TFT 2020

**Nombre y apellidos del solicitante:** Paula García Fernández

**Nombre y apellidos del tutor y en su caso, del ponente Modalidad (TFG ó TFM):** Víctor A. Villagrà

**Título del trabajo:** *DESARROLLO DE UN ENTORNO PARA LA GESTIÓN Y EL TRATAMIENTO DINÁMICO DE INTELIGENCIA DE AMENAZAS, RIESGOS Y ANOMALÍAS*

**Fecha de defensa y calificación obtenida:** 07/07/20, Calificación: 10

## RESUMEN

*Las organizaciones han ido incrementando con el paso de los años los sistemas de información que las componen. Gracias al Big Data y Cloud Computing, incorporan nuevas funcionalidades en sus sistemas y redes de comunicación. El aumento del número de datos procesados y la complejidad de los sistemas, evidencia una relación de dependencia entre el número de sistemas de una organización y los procesos de seguridad relacionados con estos. Además, con el Internet of Things, el análisis y la gestión de riesgos se convierten en procesos complicados y complejos, que van más allá de la gestión estática de riesgos. La interconexión entre millones de dispositivos pone a disposición de los atacantes la posibilidad de explotar nuevas vulnerabilidades y conlleva a la aparición de nuevas amenazas y riesgos.*

*Todas estas novedades tecnológicas requieren investigar mecanismos para hacer frente a los incidentes. Organizaciones gubernamentales desarrollan proyectos de I+D+I para investigar nuevas metodologías que incluyan estas novedades para el procesamiento y automatización y que reducen el tiempo de análisis y respuesta. En concreto, la DGAM desde hace años lleva a cabo un programa llamado COINCIDENTE para el desarrollo de soluciones tecnológicas que satisfacen una necesidad real del Ministerio de Defensa. Este trabajo se incluye dentro del proyecto PLICA perteneciente a este programa.*

*Por otro lado, esta evolución de la tecnología conlleva al avance de las amenazas que cada vez son más sofisticadas y difíciles de detectar. La aparición de nuevas amenazas, como las amenazas persistentes avanzadas APTs, ha provocado una necesidad de mejora en los procesos de detección, prevención y respuesta frente a las amenazas y de análisis de riesgos de las organizaciones. Esto afecta sobre todo a aquellas relacionadas con los sistemas gubernamentales, puesto que las APTs son ataques organizados con objetivos claros y estudiados. Es evidente la necesidad de un cambio en la manera de evaluar el riesgo al que están expuestas dado que el dinamismo de las ciberamenazas deja obsoletos los actuales sistemas de seguridad.*

*Este cambio de enfoque de los atacantes provoca que ya no sea solo necesario detectar amenazas, sino comprender cómo es su comportamiento. Por ello, adquiere gran importancia el análisis de las técnicas, tácticas y procedimientos, TTPs, de los atacantes. Esta manera de actuar frente a las amenazas permitirá generar una conciencia cibersituacional más realista y en tiempo real, más conforme a la dinámica de los sistemas actuales.*

*En la actualidad existen distintas herramientas con muchas funcionalidades para detectar y prevenir amenazas. El dinamismo de las amenazas hace imprescindible la información que se tiene de ellas. Sin embargo, dicha información debe ser analizada adecuadamente, ya que de lo contrario no genera beneficios en la lucha contra las amenazas.*

*En este contexto surgen las ontologías como sistemas expertos que permiten la representación formal de toda esa información en una estructura común. Las ontologías permiten integrar información de distintos formatos y sintaxis y son de gran utilidad en entornos heterogéneos.*

*Este trabajo pretende consolidar una serie de recursos y herramientas en un sistema integrado de datos heterogéneos con el fin de relacionar distintos tipos de información: inteligencia de amenazas,*

*anomalías y datos relacionados con la gestión de riesgos. El trabajo realiza un estudio del estado actual de los sistemas de seguridad, en cuanto a lo que la gestión de riesgos e inteligencia de amenazas se refiere, y analiza los distintos lenguajes y herramientas disponibles para la definición de ontologías y métricas de seguridad.*

*Se propone el uso de ontologías y se define una ontología final mediante el lenguaje OWL y una base de conocimiento formada por tres ontologías que van a permitir integrar información sobre*

*gestión de riesgos, inteligencia de ciberamenazas (CTI) y anomalías. Esa información debe de ser estructurada formalmente en una estructura común y mediante un lenguaje formal. El uso del lenguaje formal es fundamental para que la información tenga un sentido semántico y sea legible por máquinas. El lenguaje OWL permite definir la información que se recoge en la ontología ofreciendo una gran expresividad y un vocabulario más complejo que los anteriores lenguajes de definición de ontologías como RDFS. Para la definición de los datos de inteligencia de amenazas (CTI) se propone el uso del lenguaje STIX, ya que facilita la integración de otros esquemas y el intercambio de información CTI bajo un mismo estándar.*

*Los procesos que sigue el sistema implementado son lo más automáticos posibles para poder dar una respuesta en tiempo real o en casi tiempo real. Para ello, se ha desarrollado el sistema junto a un programa en Java que automatiza la integración de información escuchando la llegada de nuevos datos. Además, el proceso que se sigue en este sistema de seguridad retroalimenta el sistema a medida que se descubre información de amenazas y mejora la detección, la gestión y la respuesta frente a riesgos, amenazas y anomalías.*

*Por otro lado, la información que llega al sistema debe ser información veraz y coherente y en la que se pueda confiar. Además, cuanta más información se tenga, más conocimiento sobre las ciberamenazas y el sistema genera una respuesta más proactiva. Puesto que las amenazas producen consecuencias similares en organizaciones semejantes, es importante destacar la necesidad de compartir información de ciberamenazas y es por ello por lo que se propone el uso de lenguajes estándar como los mencionados anteriormente.*

*El sistema implementado integra información de fuentes externas. Dichas fuentes son: sistemas de procesamiento de Machine Learning propios de una organización para el análisis de anomalías, fuentes CTI como pueden ser otras organizaciones con las que se comparta una red para el intercambio de información de ciberamenazas e información procedente de la herramienta PILAR, desarrollada por el CCN, para la integración de la información sobre los activos en el sistema.*

*Esta información es procesada mediante reglas y motores de inferencia. Las reglas se han definido mediante el lenguaje SWRL y el motor de inferencia elegido para este trabajo ha sido Pellet. El motor de inferencia es un razonador semántico que infiere nuevo conocimiento a partir de las reglas y la información definida en la ontología.*

*Por último, el sistema es capaz de calcular el riesgo dinámicamente. Para ello, se ha desarrollado un programa en Java utilizando OWL API. El resultado de este cálculo son los riesgos residuales y potenciales a los que se expone la organización, además de propuestas de estrategias para la toma de decisiones. Para facilitar la interpretación de los resultados se ha desarrollado una interfaz gráfica donde se visualizan gráficos sobre la evolución del riesgo, que podrían simular el mando de control de un sistema de seguridad. Además, una vez obtenidos los resultados se ofrecen estrategias de actuación frente a cada uno de los riesgos.*

*El valor de este trabajo reside en la consolidación de distintos recursos y herramientas en un sistema. Gracias a la implementación de este sistema integrado se consigue gestionar un entorno heterogéneo y elaborar un mismo mecanismo de acceso y tratamiento a la información de amenazas.*

*De esta manera, se ofrece una visión global del estado y compromiso del sistema y sirve para dar soporte a la conciencia situacional en tiempo real. Además, para el desarrollo del sistema se ha hecho uso de herramientas de software libre y tecnologías actuales, gracias a las cuales pueden realizarse en el futuro pruebas y mejoras de su funcionamiento.*

## RELEVANCIA

*El trabajo de fin de máster que aquí se presenta tiene una gran relevancia en el panorama de la ciberseguridad. En concreto, los resultados de este trabajo están siendo utilizados en el proyecto PLICA (Plataforma Integrada de Conciencia Cibernética) el cual se está desarrollando dentro de uno de los programas de la DGAM.*

*Este trabajo presenta un **carácter innovador** para el conjunto de la Defensa y las Fuerzas Armadas, ya que, dentro del proyecto mencionado, se encuentra en un módulo en el que se aplican tecnologías de aprendizaje automático. Los resultados de este trabajo están siendo utilizados en el proyecto PLICA y contribuyen a la gestión y tratamiento **dinámico** de indicadores de los niveles de riesgo de la organización.*

*El trabajo conlleva una **mejora en los procesos de gestión y tratamiento de riesgos** ya que los datos se introducen en una estructura común donde la información tiene sentido semántico. Esto se consigue gracias al uso de ontologías. El sistema es inteligente y autónomo y puede analizar la información del entorno en **tiempo real** y calcular el riesgo **dinámicamente**, de modo que se reduce considerablemente el tiempo de detección de las amenazas.*

*Este trabajo tiene una gran capacidad de **integración** con otras herramientas que ya están siendo utilizadas por los sistemas de Seguridad y Defensa del Ministerio de Defensa. Gracias a ello el sistema puede interoperar con herramientas como las relacionadas con gestión de riesgos como PILAR. Esto es especialmente relevante para que los usuarios sean capaces de analizar en poco tiempo el estado del entorno, así se reduce el tiempo de respuesta y el error humano.*

*Cabe destacar que este trabajo sirve como referencia para el sistema que se está desarrollando en el Proyecto PLICA, el cual se describe con mayor detalle en el siguiente apartado, por lo que tiene una continuidad de desarrollo en el futuro.*

*Por todo lo expuesto, considero que este trabajo posee los requisitos suficientes para generar un impacto positivo para los servicios de Defensa y Seguridad en el ámbito de análisis, gestión y tratamiento de información de amenazas, riesgos y anomalías. Aporta coherencia a dicha información y contribuye a dar una respuesta proactiva ante incidentes.*

## INDICIOS DE CALIDAD

*El Trabajo de Fin de Máster DESARROLLO DE UN ENTORNO PARA LA GESTIÓN Y EL TRATAMIENTO DINÁMICO DE INTELIGENCIA DE AMENAZAS, RIESGOS Y ANOMALÍAS está estrechamente relacionado con los siguientes trabajos/proyectos:*

**Proyecto PLICA (Plataforma Integrada de Conciencia Cibernética).** El trabajo TFM se enmarca en un proyecto más amplio, llamado proyecto PLICA. Este proyecto pertenece al programa COINCIDENTE de la DGAM para proyectos de I+D+I. Dicho proyecto tiene como objetivo principal diseñar, desarrollar y validar un prototipo de Plataforma Avanzada de Conciencia Cibernética que monitorice múltiples fuentes de información heterogéneas, procese datos recolectados mediante técnicas de aprendizaje automático y sistemas expertos, y sea capaz de detectar y predecir patrones avanzados de ataques, así como de estimar el riesgo de exposición de los mismos.

*Para ello, se lleva a cabo la integración de sensores de presencia basados en la monitorización de capacidades de conectividad de dispositivos ya sea Telefonía Móvil 2G, 3G o 4G, tecnología Bluetooth, tecnología WiFi o señales de radiofrecuencia (RF), de especial relevancia por la ubicuidad de estas tecnologías. El resultado del proyecto es un prototipo de nivel TRL 6 que se valida en un demostrador tecnológico en los entornos militares del MCCD (Mando Conjunto de CiberDefensa).*

*El sistema diseñado en este TFM se utiliza en el proyecto PLICA por lo que se considera que es un trabajo que tiene una continuidad en el tiempo y sirve de base para el desarrollo del sistema final de dicho proyecto.*

**Tesis Doctoral de Raúl Riesco Granadino, “Contribution to dynamic risk management automation by an ontology- based framework”, E.T.S.I. Telecomunicación (UPM), año 2019.** Raúl Riesco Granadino es el Gerente de I+D+i y Promoción del Talento en el Instituto Nacional de Ciberseguridad (INCIBE) y copresidente del “Grupo de Trabajo 3 - I+D+i en seguridad TIC” de la Plataforma NIS de la Comisión Europea. La tesis elaborada por el mismo en 2019 propone un marco para la Gestión y Evaluación Dinámica de Riesgos (DRM/ DRA) y promueve el intercambio de información de ciberamenazas, CTI. Para ello, implementa una ontología híbrida de riesgos (DRM) y amenazas (CTI), basada en el lenguaje OWL y el formato STIX.

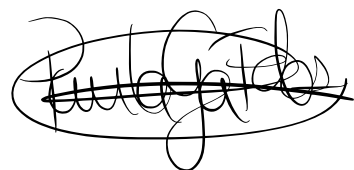
El trabajo TFM que se somete a este concurso está relacionado íntimamente con la tesis doctoral de Raúl Riesco Granadino puesto que es una continuación de la misma. El trabajo TFM incluye el estudio y lectura de esta tesis para posteriormente completar su contribución añadiendo nuevas funcionalidades. La ontología que se define en el trabajo TFM recoge esa ontología híbrida, la actualiza y la adapta añadiendo una nueva para integrar datos sobre anomalías. Las ontologías que se detallan en la tesis son extendidas con otras funcionalidades que se explican detalladamente en el trabajo para una respuesta frente amenazas en tiempo real.

Cabe destacar que también existen otros trabajos relacionados con el desarrollo de este sistema, como el Trabajo de Fin de Máster de Carmen Sánchez Zas (“Design of an adaptable real-time Machine Learning Intrusion Detection System based on attacks categorization”) cuyo sistema aporta los datos que se tratan en este TFM y el de Trabajo de Fin de Grado de Melisa Anahi Maccio Parigino (“Diseño y Validación de una Ontología y Reglas Formales de Comportamiento para una aplicación de Conciencia Cibernética”), cuyas reglas toman como base el sistema desarrollado en este trabajo que somete a concurso.

## REFRENDO

El abajo firmante se hace responsable de la veracidad de los datos contenidos en esta solicitud. Asimismo, entiende que su presentación a la convocatoria lleva aparejada la cesión a la Cátedra ISDEFE-UPM en Defensa y Seguridad del derecho a publicar en sus medios de difusión este resumen. Asimismo, en el caso de que resulte agraciado con uno de los premios, cede a la Cátedra el derecho de hacer público este hecho.

Madrid 3 de enero de 2021



Fdo: Paula García Fernández  
DNI: 05291814C