Fecha del CVA	20/04/2018

Parte A. DATOS PERSONALES

Nombre y apellidos	Jesús E. Díaz Verdejo		
DNI/NIE/pasaporte	52573664B	Edad	51
Núm. identificación del investigador	Researcher ID	B-5372-2011	
	Código Orcid	0000-0002-8424-9932	

A.1. Situación profesional actual

Organismo	Universidad de Granada			
Dpto./Centro	Teoría de la Señal, Telemática y Comunicaciones			
Dirección	c/ Daniel Saucedo Aranda, s/n			
Teléfono	958242304	Correo electrónico	jedv@ugr.es	
Categoría profesional	Catedrático de Universidad		Fecha inicio	3/12/2011
Espec. cód. UNESCO	*1203.10, 1203.17, 3325.99 (telemática)*			
Palabras clave	Ingeniería Telemática, Seguridad en redes, Detección de intrusiones, Ingeniería de tráfico			

A.2. Formación académica *(título, institución, fecha)*

Licenciatura/Grado/Doctorado	Universidad	Año
Licenciado Ciencias Físicas	Granada	1989
Doctor Ciencias Físicas	Granada	1995

A.3. Indicadores generales de calidad de la producción científica *(véanse instrucciones)*

- *Sexenios de investigación: 4, el último concedido en 2015*
- *3 tesis doctorales dirigidas en los últimos 10 años.*
- *Publicaciones indexadas: 44 (Wos), 52 (Scopus)*
- *Citas totales: 590 (WoS), 966 (Scopus)*
- *Promedio citas (últimos 5 años): 86 citas/año, (WoS), 127 citas/año (Scopus)*
- *Publicaciones JCR: Q1: 7, Q2: 11, Q3: 3, Q4: 3*
- *Índice h: 10 (WoS), 13 (Scopus)*

Parte B. RESUMEN LIBRE DEL CURRÍCULUM

Jesús E. Díaz Verdejo es Catedrático de Universidad de *Ingeniería Telemática* de la Universidad de Granada, adscrito al Dpto. de Teoría de la Señal, Telemática y Comunicaciones.

Su labor investigadora y docente se centra en el campo de las redes y las comunicaciones, especialmente en el ámbito de la *seguridad en redes y sistemas*, sin excluir otros aspectos como la tele-enseñanza, la ingeniería de tráfico y las aplicaciones telemáticas. Su línea principal de investigación está orientada al análisis y modelado de actividades y eventos para la detección de incidentes de seguridad y la respuesta a los mismos, tanto mediante detección de anomalías como mediante técnicas híbridas. También, con una orientación a la seguridad de las comunicaciones y redes, ha desarrollado trabajos en el ámbito de la identificación de tráfico de red y la correlación de alertas. En todos estos campos ha aplicado conocimientos y técnicas relativas al aprendizaje automático y la minería de datos, el modelado de procesos mediante modelos de Markov y el análisis y modelado de protocolos de comunicaciones. Con anterioridad, desarrolló su investigación en el procesamiento y reconocimiento de voz, en el que también ha realizado contribuciones significativas.

Su actividad investigadora es extensa y de impacto internacional, tal y como se puede juzgar del currículum completo, en el que se consignan las diferentes aportaciones. Así, en

su currículum se recogen una veintena de libros y capítulos de libro, alrededor de medio centenar de publicaciones en revistas internacionales de reconocido prestigio y en torno a 70 contribuciones en congresos nacionales e internacionales. Ha dirigido 6 tesis doctorales, 4 de ellas en el campo de la seguridad en redes.

Ha participado como investigador en 22 proyectos: 11 del Plan Nacional de I+D, 1 proyecto del VI programa marco de la UE y 11 contratos de transferencia de investigación. De entre éstos, ha sido investigador principal de dos proyectos del Plan Nacional de I+D y 3 contratos de transferencia de tecnología; correspondiendo la mayor parte de las publicaciones científicas mencionadas con anterioridad a la publicación de los resultados de estos proyectos.

Es editor de "Security and Communication Networks (ISSN: 1939-0122, IF 1,067 (Q4)) y revisor de numerosas revistas científicas y congresos internacionales y nacionales, evaluador de proyectos, organizador de diversas reuniones y actividades técnicas, además de miembro del *CITIC-UGR*. Desde 2017 está adscrito al grupo TIC154 del PAIDI.

Su carrera se encuentra marcada por su participación activa en la implantación del área de IT y la titulación de Ing. de Telecomunicación en la Univ. de Granada.

En el contexto de la seguridad en redes, ha desarrollado sistemas de detección de intrusiones (IDS), especialmente para sistemas web, de los que existen demostradores, habiendo dado lugar a contratos de transferencia. También ha desarrollado técnicas para la clasificación de flujos y para correlación de alertas y eventos en entornos de monitorización de red. En ambos casos existen prototipos operativos.

Su objetivo a medio/largo plazo es consolidar la línea de investigación en seguridad, desarrollando soluciones reales y efectivas, que puedan ser objeto de transferencia, para la prevención y respuesta a intrusiones así como la monitorización de la seguridad de las redes.

Parte C. MÉRITOS MÁS RELEVANTES *(ordenados por tipología)*

C.1. Publicaciones

- Saeed Salah, Gabriel Maciá-Fernández, Jesús E. Díaz-Verdejo, **Fusing information from tickets and alerts to improve the incident resolution process**, Information Fusion, 45:38-52, 2018. ISSN: 1566-2535. Ranking: 4/104 (Q1)
- Saeed Salah, Gabriel Maciá-Fernández, Jesús E. Díaz-Verdejo, Leovigildo Sánchez-Casado, "**A Model for Incident Tickets Correlation in Network Management",** Journal of Network and Systems Management, 24:57-91, 2016. ISSN: 1064-7570. Ranking: 48/89 (Q3)
- Amjad Hajjar, Jawad Khalife, Jesus Diaz-Verdejo, "**Network Traffic Application Identification Based on Message Size Analysis",** *Journal of Networks and Computer Applications* 58:130-143, 2015. ISSN: 1084-8045. Ranking: 7/104 (Q1)
- Pedro García-Teodoro. Jesús E. Díaz-Verdejo, Juan M. Tapiador, Rolando Hernandez-Salazar, "**Automatic Generation of HTTP Intrusion Signatures by Selective Identification of Anomalies**", *Computers & Security*, 55:159-174, 2015. ISSN: 0167-4048. Ranking: 69/139 (Q2)
- José Camacho, Pablo Padilla, Pedro Garcìia-Teodoro, Jesús Díaz-Verdejo, **"A Generalizable Dynamic Flow Pairing Method for Traffic Classification**", *Computer Networks*, 57:2718-2732, 2013. ISSN: 1389-1286. Ranking: 17/50 (Q2)
- Saeed Salah, Gabriel Maciá-Fernández, Jesús E. Díaz-Verdejo, "**A Model-based Survey of Alert Correlation Techniques**", Computer Networks, 57:2718-2732, 2013. ISSN 1389-1286. Ranking: 17/50 (Q2)
- Francisco Salcedo-Campos, Jesús Díaz-Verdejo, Pedro García-Teodoro, **"Segmental parameterisation and statistical modelling of e-mail headers for spam detection**", *Information Sciences*, 195:45-61, 2012, ISSN: 0020-0255. Ranking: 6/132 (Q1)
- José Camacho, Pablo Padilla, Jesús Díaz-Verdejo, Keith Smith, David Lovett, "**Least-squares Approximation of a Space Distribution for a given Covariance and Latent**

Sub-space", *Chemometrics and Intelligent Laboratory Systems*, 105:171-180, 2011, ISSN: 0169-7439. Ranking: 12/58 (Q1)

- Gabriel Maciá-Fernández, Pedro García-Teodoro, Jesús Díaz-Verdejo, "**Mathematical Model for Low-Rate DoS Attacks Against Application Servers**", IEEE Trans. on Information Forensics And Security, 4:519-529, 2009. ISSN 1556-6013. Ranking: 10/92 (Q1)
- P. Garcia-Teodoro, J. Diaz-Verdejo, G. Macia-Fernandez, E. Vazquez, "**Anomaly-based network intrusion detection: Techniques, systems and challenges**", *Computers & Security*, 28:18-28, 2009, ISSN: 0167-4048. Ranking: 48/116 (Q2). Artículo más descargado de la publicación durante el año 2013. 314 citas en WoS, 493 en Scopus.

C.2. Proyectos

1. Referencia del proyecto: TEC2011-22579
   Título: SuMA: **Supervivencia de Redes MANET ante Incidentes de Seguridad**
   Investigador principal: Pedro García Teodoro (Univ. de Granada)
   Entidad financiadora: MICINN
   Duración: 01/01/2012-31/12/2014
   Financiación recibida (en euros): 56265 €
   Participación: Investigador

2. Referencia del proyecto: TEC2008-06663-C03-02
   Título: **Seguridad del entorno en redes Peer-to-Peer**
   Investigador principal: Jesús E. Díaz Verdejo (Univ. de Granada)
   Entidad financiadora: MCI
   Duración: 01/01/2009-31/12/2011
   Financiación recibida (en euros): 56386 €
   Participación: Investigador principal

3. Referencia del proyecto: TSI2005-08145-C02-02
   Título: **Modelo de Arquitectura por Capas para la Detección Ubicua de Ataques y Respuesta**
   Investigador principal: Pedro García Teodoro (Univ. de Granada)
   Entidad financiadora: MCYT
   Duración: 31/12/2005-31/12/2008
   Financiación recibida (en euros): 60000 €
   Participación: Investigador

4. Referencia del proyecto: EUREKA-CELTIC (CP3-011)
   Título: **RED: Reaction After Detection**
   Investigador principal: Enrique Vázquez Gallo (UPM)
   Entidad financiadora: EUREKA-CELTIC
   Duración: 1/1/2007-31/12/2007
   Financiación recibida (en euros):
   Participación: Investigador

C.3. Contratos, méritos tecnológicos o de transferencia

1. Referencia del proyecto: PI-1736/22/2017
   Título: **Detección Temprana de Ataques de Ciberseguridad en Servidores Web de la biblioteca de la US**
   Investigador principal: Rafael Estepa Alonso (Univ. de Sevilla)
   Entidad financiadora: Universidad de Sevilla
   Duración: 01/01/2017 – 30/09/2018
   Financiación recibida (en euros):

2. Título: **Sistema Integral para Vigilancia y Auditoría de Ciberseguridad Corporativa**
   Investigador principal: Rafael Estepa Alonso (Univ. de Sevilla)
   Entidad financiadora: Wellness Telecom, S.L / Corporación Tecnológica de Andalucía
   Duración: 01/04/2017-31/12/2019
   Financiación recibida (en euros): 79200 €
   Participación: Investigador

3. Título: **Investigación sobre fraude en telecomunicaciones. El fraude en roaming**
Investigador principal: Gabriel Maciá Fernández (Univ. de Granada)
Entidad financiadora: KPN Mobile International Network Spain S.L.
Duración: 15/04/2013-15/04/2014
Financiación recibida (en euros): 12223.9 €
Participación: Investigador

4. Título: **Mejora de la gestión de red mediante análisis y caracterización del tráfico en redes corporativas**
Investigador principal: Gabriel Maciá Fernández (Univ. de Granada)
Entidad financiadora: SADESI (Junta de Andalucía)
Duración: 01/07/2010-30/06/2011
Financiación recibida (en euros): 25056 €
Participación: Investigador

5. Título: **Tele-rehabilitación efectiva en el hogar: investigación y desarrollo de sistemas, técnicas, métodos y mecanismos (TeleREHAB)**
Investigador principal: Pedro García Teodoro (Univ. de Granada)
Entidad financiadora: Fundación Robotiker
Duración: 15/04/2009-15/04/2011
Financiación recibida (en euros): 69600 €
Participación: Investigador

C.4. Patentes

C.5, C.6, C.7… Otros

- IP de dos proyectos nacionales y 3 contratos de transferencia.
- Premio a la Excelencia Docente 2009 de la Universidad de Granada.
- Editor de “Security and Communication Networks (ISSN: 1939-0122, IF 1,067 (Q4))
- Revisor de las revistas: Neural Processing Letters, IEEE Systems, Man & Cybernetics, IEEE Communication Letters, Information Sciences (Elsevier), IEEE Trans. On Information Forensics and Security, Knowledge and Information Systems, KSII Transactions on Internet and Information Systems, Computer Networks, International Journal of Information Security, Computers & Security, IEEE Transactions on Network and Service Management.
- Revisor de los congresos: ICANN, JITEL, WICS, ICICS, AP2PS, CISIS, NSS, CSS.
- Miembro del comité de programa de los congresos: WICS05, JITEL (eds. 2008 a 2013), AP2PS (2010 y 2011)
- Comité organizador de NATO-ASI93, JITEL’13 y ASTROROB’04
- Revisor de ANEP
- Desarrollador del sistema STACC (Sistema Telefónico Automático de Consulta de Calificaciones) que estuvo operativo varios años en el DETC de la UGR. Este sistema fue presentado en varios congresos y atendió miles de llamadas usando reconocimento de voz durante el periodo 1997-1999.
- Ha intervenido de forma activa en el diseño y elaboración de la base de datos “Albaycin”, subvencionada por la CICYT, en colaboración con otras universidades españolas, realizando labores de investigador principal. Fruto de este trabajo han resultado varios informes y comunicaciones presentadas a varios congresos y una base de datos de voz ampliamente usada en investigación, distribuida a través de ESCA.
- Director de más de 40 proyectos fin de carrera en las titulaciones de Ing. Electrónica, Ing. Informática e Ing. Telecomunicación
- Premio a la mejor tesis doctoral en Comercio Electrónico 2008, Colegio Oficial de Ingenieros de Telecomunicación: "Ataques de Denegación de Servicio a Baja Tasa contra Servidores" (Co-director de la tesis).