CURRICULUM VITAE ABREVIADO (CVA)

Fecha del CVA	18/06/2024

Parte A. DATOS PERSONALES

Nombre	*Jesús Esteban*		
Apellidos	*Díaz Verdejo*		
Sexo (*)	*M*	Fecha de nacimiento (dd/mm/yyyy)	-
DNI, NIE, pasaporte	-		
Dirección email		URL Web	
Open Researcher and Contributor ID (ORCID) (*)	*0000-0002-8424-9932*		

** datos obligatorios*

A.1. Situación profesional actual

Puesto	*Catedrático de Universidad*		
Fecha inicio	*2011*		
Organismo/ Institución	*Universidad de Granada*		
Departamento/ Centro	*Teoría de la Señal, Telemática y Comunicaciones*		
País	*España*	Teléfono	-
Palabras clave	*Ingeniería Telemática, seguridad en redes, detección de intrusiones, detección de anomalías, ingeniería de tráfico*		

A.2. Situación profesional anterior (incluye interrupciones en la carrera investigadora, de acuerdo con lo indicado en la convocatoria, indicar meses totales)

Periodo **Puesto/ Institución/ País / Motivo interrupción**

01/01/90–30/09/90 Becario PFPI / Universidad de Granada / Esp
01/10/90–30/09/92 Profesor Asociado T1 / Universidad de Granada / Esp
01/10/92–30/11/95 Profesor Asociado T2 / Universidad de Granada / Esp
01/12/95–24/03/97 Profesor Asociado T3 / Universidad de Granada / Esp
25/03/97–30/03/98 Profesor Titular Interino / Universidad de Granada / Esp
1/4/1998–2/12/2011 Profesor Titular Univ. / Universidad de Granada / Esp

A.3. Formación Académica

Grado/Master/Tesis	**Universidad/Pais**	**Año**
Licenciado en Ciencias Físicas	*Granada*	*1989*
Doctor en Ciencias Físicas	*Granada*	*1995*

Parte B. RESUMEN DEL CV *(máx. 5.000 caracteres, incluyendo espacios)*

Jesús E. Díaz Verdejo es Catedrático de Universidad de Ingeniería Telemática en el Departamento de Teoría de Señal, Telemática y Comunicaciones de la Universidad de Granada.

Su labor investigadora y docente se centra en el ámbito de las redes y las comunicaciones, especialmente en el ámbito de la seguridad de redes y sistemas, sin excluir otros aspectos como la ingeniería de tráfico o las aplicaciones telemáticas. Su principal línea de investigación está orientada al análisis y modelización de actividades y eventos para la detección de incidentes de seguridad y la respuesta a los mismos, tanto mediante la detección de anomalías como mediante el uso de técnicas híbridas. Asimismo, con una orientación a la seguridad de las comunicaciones y redes, ha desarrollado trabajos en el campo de la

identificación del tráfico de red y la correlación de alertas y eventos. En todos estos campos ha aplicado conocimientos y técnicas relacionadas con el aprendizaje automático y la minería de datos, la modelización de procesos mediante modelos de Markov, el análisis de series temporales y el análisis y modelización de protocolos de comunicación. Anteriormente, desarrolló su investigación en procesamiento y reconocimiento del habla.

Su actividad investigadora es extensa y de impacto internacional, como se desprende del su CV. Así, en su currículum se recogen veinte libros y capítulos de libros, alrededor de medio centenar de publicaciones en revistas internacionales de prestigio, la mayoría indexadas en WoS, y alrededor de un centenar de contribuciones en congresos nacionales e internacionales, todos ellos con revisión por pares. Ha dirigido 6 tesis doctorales, 4 de ellas en el ámbito de la seguridad de redes. Ha participado como investigador en 35 proyectos: 15 del Plan Nacional y Regional de Investigación y Desarrollo, 1 proyecto del 6º programa marco de la UE y 19 contratos de transferencia de investigación. Entre ellos, ha liderado 4 proyectos del Plan Nacional de Investigación y Desarrollo y 3 contratos de transferencia de tecnología. Es revisor de numerosas revistas y congresos científicos internacionales y nacionales, evaluador de proyectos, organizador de diversos encuentros y actividades técnicas, así como miembro del CITIC-UGR. Desde 2017 está adscrito al grupo de investigación TIC154 de PAIDI, desarrollando una línea de investigación en ciberseguridad. Sus indicadores bibliométricos en WoS son: 55 publicaciones, 1599 citas e índice h=15.

En el contexto de la seguridad de redes, ha desarrollado sistemas de detección de intrusos (IDS), especialmente para sistemas web, para los que existen prototipos que han sido objeto de acciones de transferencia. También ha desarrollado técnicas para la clasificación de flujos y para la correlación de alertas y eventos en entornos de monitorización de redes, con especial foco en entornos industriales e IoT, para los que también se han generado prototipos operativos y herramientas de dominio público.

Su objetivo a medio/largo plazo es consolidar la línea de investigación en seguridad, desarrollando soluciones reales y efectivas que puedan ser transferidas, tanto para la prevención y respuesta a intrusiones como para la monitorización de la seguridad de la red. En la actualidad investiga en la detección de anomalías en los comportamientos de los usuarios (UEBA) como elemento para la detección de ciberataques.

Parte C. LISTADO DE APORTACIONES MÁS RELEVANTES

C.1. Publicaciones más importantes en libros y revistas con “peer review” y conferencias (indicadores según WoS, se incluyen las más relacionados con ciberseguridad de mayor impacto)

- Vicente Mayor, Agustín Lara, Rafael Estepa, Antonio Estepa, Jesús E. Diaz-Verdejo, **Smart Home Anomaly-based IDS: Architecture Proposal and Case Study**, Internet of Things, (22)100773, 2023. doi: 10.1016/j.iot.2023.100773. **Q1, 5 citas** (2,5/año).
- Díaz-Verdejo, J.; Muñoz-Calle, J.; Estepa Alonso, A.; Estepa Alonso, R.; Madinabeitia, G., **On the Detection Capabilities of Signature-Based Intrusion Detection Systems in the Context of Web Attacks**, Applied Sciences, (12)852, 2022. Doi: 10.3390/app12020852. **Q2, 17 citas** (5,7/año)
- Jesús Díaz-Verdejo, Antonio Estepa, Rafael Estepa, German Madinabeitia, Fco. Javier Muñoz, **A methodology for conducting efficient sanitization of HTTP training datasets**, Future Generation Computer Systems, (109)67-82, 2020. Doi: 10.1016/j.future.2020.03.033 **Q1, 5 citas** (1/año).
- Rafael Estepa Alonso, Jesús Díaz-Verdejo, Antonio Estepa Alonso, Germán Madinabeitia, **How much training data is enough?. A case study for HTTP anomaly-based intrusion detection,** IEEE Access, (8)44410-44425, 2020. Doi: 10.1109/ACCESS.2020.2977591. **Q1, 8 citas** (1,6/año)

- S. Salah, G. Maciá-Fernández, J. E. Díaz-Verdejo, **Fusing information from tickets and alerts to improve the incident resolution process**, Information Fusion, 45:38-52, 2019. Doi: 10.1016/j.inffus.2018.01.011. **Q1, 5 citas** (0,8/año)
- 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. Doi: 10.1016/j.jnca.2015.10.003. **Q1, 20 citas** (2/año)
- Pedro García-Teodoro. Jesús E. Díaz-Verdejo, Juan M. Tapiador, Rolando HernandezSalazar, "**Automatic Generation of HTTP Intrusion Signatures by Selective Identification of Anomalies**", Computers & Security, 55:159-174, 2015. Doi: 10.1016/j.cose.2015.09.007. **Q2, 17 citas**, (1,7/año)
- Jawad Khalife, Amjad Hajjar, Jesús Díaz-Verdejo, **A Multilevel Taxonomy and Requirements for an Optimal Traffic-classification Model,** Int. Journal of Network Management, 24(2):101-120, 2014. Doi: 10.1002/nem.1855. **Q4, 36 citas** (3,27/año)
- Saeed Salah, Gabriel Maciá-Fernández, Jesús E. Díaz-Verdejo, "**A Model-based Survey of Alert Correlation Techniques**", Computer Networks, 57:2718-2732, 2013. Doi: 10.1016/j.comnet.2012.10.022. **Q2, 90 citas** (7,5/año)
- 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. Doi: 10.1016/j.cose.2008.08.003. **Q2, 955** citas (60/año)

C.3. Proyectos o líneas de investigación en los que ha participado. *Se incluyen los 5 recientes más relacionados con ciberseguridad.*

1. **Modelado de Ataques y Detección de Incidentes de Ciberseguridad (**A-TIC-224UGR20)
   Inv. principal: Jesús E. Díaz Verdejo / Juan Carlos Cubero Talavera
   Entidad: Junta de Andalucía -UGR, Proyectos I+D+i del Programa Operativo FEDER 2020
   Fechas: 2021/2022
   Rol: Investigador principal
2. **Sistema para la detección temprana de ciberataques en industria conectada e IoT mediante detección de anomalías multiplanta** (2020/00000172)
   Inv. principal: Rafael Estepa Alonso (Univ. de Sevilla)
   Entidad: Junta de Andalucía -UGR, Proy. I+D+i Programa Operativo FEDER 2020 – CEI20
   Fechas: 2021/2022
   Rol: Investigador
3. **Detección de ciberataques en industria conectada e IoT mediante integración y correlación de alertas multifuente** (PID2020-115199RB-I00)
   Inv. principal: Jesús E. Díaz Verdejo / Juan Carlos Cubero Talavera
   Entidad: Ministerio de Ciencia e Innovación
   Fechas: 2021/2024
   Rol: Investigador principal
4. **Detección Inteligente de Incidentes de Ciberseguridad en redes IoT en base a ngramáticas adaptativas (Intelligent detection of cybersecurity incidents in IoT netwokrs based on adaptative n-grams) (**2020/00000172)
   Inv. principal: Rafael Estepa Alonso (Univ. de Sevilla)
   Entidad: Junta de Andalucía - FEDER
   Fechas: 2020-2021
   Rol: Investigador
5. **SuMA: Supervivencia de Redes MANET ante Incidentes de Seguridad** (TEC201122579)

Inv. principal: Pedro García Teodoro (Univ. de Granada)
Entidad: MICINN
Fechas: 01/01/2012-31/12/2014
Rol: Investigador

C.4. Participación en actividades de transferencia de tecnología/conocimiento y explotación de resultados

Contratos de transferencia *(los 5 más recientes relacionados con ciberseguridad)**:*** *- PI-2437/22/2023 -* ***Solución integral de Gestión de Identidades de Nueva Generación (OREOS)***
Entidad financiadora: WHITEBEARSOLUTIONS S.L.
Inv. principal: Rafael Estepa Alonso (Univ. de Sevilla)
Empresa: WHITEBEARSOLUTIONS S.L. / Periodo: 2023 – 2025 / Rol: Investigador

- *PI-2132/22/2021 –* ***Detección de ciberamenazas en los sistemas de monitorización y control de instalaciones de Generación Renovables*** *(RENSHIELD).*
  Entidad financiadora: Isotrol / Ministerio Ciencia y Tecnología (Programa CIEN)
  Inv. principal: Antonio Estepa Alonso (Univ. de Sevilla)
  Empresa: Isotrol / Periodo: 2021 – 2023 / Rol: Investigador - *PI-1814/26/2018 –* ***Red Eléctrica cibersegura 1****.*
  Entidad financiadora: Isotrol / Ministerio Ciencia y Tecnología (Programa CIEN).
  Inv. principal: Antonio Estepa Alonso (Univ. de Sevilla)
  Empresa: Isotrol / Periodo: 01/01/2018 – 31/12/2021 / Rol: Investigador
- *CTA 16/909,* ***Sistema Integral de Vigilancia y Auditoría de ciberseguridad corporativa*** *(SIVA).*
  Entidad financiadora: Wellness Telecom, Corporación Tecnológica de Andalucía.
  Inv. principal: Rafael Estepa Alonso (Univ. de Sevilla)
  Empresa: Wellness Telecom, SL / Periodo: 01/04/2017-31/12/2019 / Rol: Investigador
- *PI-1736/22/2017,* ***Detección Temprana de Ataques de Ciberseguridad en Servidores Web de la biblioteca de la US****.*
  Financiado por la Univ. de Sevilla.
  Inv. principal: Rafael Estepa Alonso (Univ. de Sevilla)
  Empresa: Universidad de Sevilla / Periodo: 01/01/2017–30/09/2018 / Rol: Investigador ***Modelos de utilidad***

- **Demostrador de anomalías en aplicaciones de iluminación inteligente,** Inventores: *Rafael Estepa Alonso, Antonio Estepa Alonso, Jesús Díaz Verdejo, Germán Madinabeitia Luque, Agustín Lara Romero* Fecha: *2023.*
  Entidad titular: *Univ. de Sevilla / Univ. de Granada*
  Empresas que lo están explotando: *Wellness Telecom, S.L.* ***Otros resultados relevantes (de dominio público)***

- ***InspectorLog***. Software para la detección de intrusiones en HTTP basada en firmas a partir de las trazas del servicio. J. Díaz-Verdejo, J. Muñoz-Calle, R. Estepa Alonso, A. Estepa Alonso. *https://gitlab.com/neus_cslab/inspectorlog*

- ***BiblioUS17***. *Dataset de peticiones HTTP reales etiquetadas para entrenamiento y validación de AIDS y WAF. Dıaz-Verdejo, Jesús E.; Estepa, Rafael; Estepa, Antonio; Muñoz, Fco. Javier; Madinabeitia, German, https://idus.us.es/handle/11441/148254, doi: 10.12795/11441/148254*