

# DANIEL DÍAZ LÓPEZ



Móvil (57) 3006643625

Email: [daniel.diaz@escuelaing.edu.co](mailto:daniel.diaz@escuelaing.edu.co)

Web: <http://webs.um.es/felixgm/pubs/managing-access-control-systems-in-distributed-environments-with-dynamic-asset-protection/>

---

## PERFIL PROFESIONAL

Doctor en Informática en la línea de Seguridad de la Información, con distinciones Cum Laude y Doctor Internacional. Ha sido miembro de los siguientes grupos de investigación: *Intelligent Systems and Telematic Research Group* de la Universidad de Murcia en España; *Security Group* de *NEC Laboratories Europe (NLE)* en Heidelberg, Alemania, Grupo de Internet y Telemática de CINTEL (Centro de Investigación y Desarrollo en TIC) en Colombia y Grupo CTG-Informática de la Escuela Colombiana de Ingeniería Julio Garavito. Es consultor en la implementación de Sistemas de Gestión de Seguridad de la Información (SGSI), Sistemas de Gestión de Continuidad de Negocio (SGCN) y Seguridad para Arquitectura Empresarial, habiendo participado en proyectos de consultoría con diferentes empresas colombianas. Daniel es Ethical Hacker Certificado (CEH), Auditor Líder ISO27001 y Auditor Interno ISO22301. Manejo de idiomas: inglés, español, portugués. Actualmente, Daniel es **profesor asistente** del programa de Ingeniería de Sistemas de la Escuela Colombiana de Ingeniería Julio Garavito e investigador del grupo CTG-Informática de la misma universidad.

Sus líneas de investigación actuales son: ciberdefensa, ciberinteligencia, privacidad, seguridad en la construcción de software, ethical hacking y seguridad para Internet de las Cosas (IoT).

---

## EXPERIENCIA LABORAL Y DE INVESTIGACIÓN

**Profesor Asistente** en [Escuela Colombiana de Ingeniería 'Julio Garavito'](#)

Agosto 2016 – Actualidad

Actualmente tengo el mejor trabajo del mundo: ¡Obtengo un pago por estudiar e investigar apasionadamente sobre temáticas relacionadas a ciberseguridad! Proponer y desarrollar proyectos de I+D relacionados con seguridad de la información, bajo el rol de Líder Técnico. Orientación de cursos: Seguridad en el Desarrollo de Software, Seguridad Informática, Sistemas de Gestión de Seguridad de la Información y otros próximamente (*Ethical Hacking*, Examinador forense). Apoyar procesos educativos internos orientados al mejoramiento continuo, fortalecimiento de relaciones con la industria/academia/sector gobierno, internacionalización y desarrollo de nuevo programas. Consejero académico de estudiantes de pregrado como agradecimiento a todos los buenos mentores que tuve a lo largo de mi carrera profesional y académica. Proyectos de investigación en los que participo actualmente:

- i. Implantación de una solución SIEM para la protección de activos de información en conjunto con la Universidad de Murcia y NEC Laboratories Europe. Rol: Investigador líder.
- ii. Plataforma para la detección en tiempo real de ataques informáticos a partir de eventos de seguridad de dispositivos de red. Rol: Asesor de proyecto de grado.
- iii. Seguridad para IoT: Solución para la gestión de eventos de seguridad en arquitecturas de Internet de las cosas (IoT). Rol: Director de proyecto de grado.
- iv. Análisis de Riesgos en Escenarios de IoT. Rol: Director de proyecto de grado.

**Consultor en Seguridad de la Información** en [Superintendencia de Industria y Comercio](#)

Mayo 2016 – Agosto 2016

Implementación de 26 controles de seguridad del Sistema de Gestión de Seguridad de la Información de la Entidad. Alineación de los objetivos de seguridad de la entidad con la Estrategia de Gobierno en Línea (Gobierno electrónico). Diseño y aplicación del procedimiento de gestión de incidentes de seguridad. Pruebas de penetración sobre sistemas de información.

**Consultor en seguridad de la información** en [Centro de Investigación y Desarrollo en TICS](#),

Octubre 2012 – Diciembre 2015

Implementación de Sistemas de Gestión de Seguridad de la Información (SGSI) bajo el estándar ISO27001, realización de pruebas de Ethical Hacking y Pruebas de penetración (OSSTMM), implementación y seguimiento de procedimientos de gestión de respuesta de incidentes a seguridad, gestión de cambios. Seguimiento a guías del PMI. Generación de declaraciones de aplicabilidad (SoA). Auditoria a SGSI, gestión de riesgos de seguridad, implementación de contramedidas contra fuga de información, generación de KPIs (Key Performance Indicators), implementación de servicios de TI siguiendo las directrices de ITIL. Líder del equipo de seguridad de la información. Alta interacción con clientes y resolución de problemas.

**Oficial de seguridad de la Información** en [Departamento para la Prosperidad Social](#)

Enero 2014 – Diciembre 2014

Dirigir la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) de la Entidad alineado con la norma NTC ISO/IEC 27001 y el Modelo de Seguridad de la Información definido por Gobierno en Línea (GEL) – Manual 3.1. Cumplir con las metas en cuanto a desarrollo de las fases planear, hacer, verificar y actuar del SGSI que permitan aumentar el índice GEL de la Entidad y lograr una protección de los activos de información para el proceso de gestión tecnológica. Definir y desarrollar controles de seguridad y contramedidas para fortalecimiento de la infraestructura tecnológica. Gestionar riesgos de seguridad. Aplicar una arquitectura de defensa en profundidad. Ethical hacking. Realizar la detección de vulnerabilidades técnicas y definir un plan de mitigación. Definición y análisis de soluciones de seguridad de diferentes proveedores.

**Investigador en Seguridad de la Información** en [NEC Laboratories Europe](#)

Noviembre 2011 – octubre 2012

Propuesta, diseño e implementación de mejoras en soluciones AAA (Authentication, Authorization, Accounting), con énfasis en sistemas distribuidos y heterogéneos utilizando tecnologías estandarizadas (XACML, SAML, HTTPS, SOAP). Desarrollo de una propuesta y prototipo para un sistema de gestión de acceso basado en riesgo (RAdAC) utilizando algoritmos bio-inspirados. Análisis e integración de sistemas de gestión de identidad SSO (OpenID, OAuth, SAML) de la compañía para su despliegue en la nube. Propuesta de aplicación de soluciones criptográficas para la preservación de la privacidad del usuario. Desarrollo de prototipos en JAVA, HTML, XML. Generación de un artículo científico con una propuesta de metodología de gestión del riesgo con aplicabilidad en ISO 27001/27005. Escritura y publicación de artículos de investigación. Estudios de productos de NEC para seguridad y gestión de identidad (NC7000).

**Ingeniero de Infraestructura** en [ITIS SUPPORT](#)

Julio 2009 – Septiembre 2010

Creación y gestión del centro de datos de la compañía para despliegues de ambientes de producción y entrenamiento de tipo CRM y HRM. Definición, implementación y mantenimiento de políticas de seguridad y tráfico de red a través de firewalls, DMZ, VPN, IDS y monitores de actividad de red. Gestión de plataformas para la entrega de servicios de telefonía (VoIP) y datos (GigaEthernet) y servicios de red (email, DHCP, DNS, FTP, Active Directory, VPN). Soporte técnico y contacto con clientes. Gestión de distribuciones de sistemas operativos servidor Linux/Windows. Especialista en seguridad de la información y técnicas de virtualización para datacenters. Gestión de sistema de seguridad electrónica: video (CCTV), control de acceso (Digiwatch), alarma de robo e incendio.

**Ingeniero Técnico** en [Universidad del Cauca](#)

Marzo 2008 – Mazo 2009

Responsable del análisis y diseño de redes de acceso de tipo inalámbricas seguras (WiMAX, WiFi) para el establecimiento de conexiones de banda ancha entre la red metropolitana de la ciudad de Popayán y locaciones remotas de la región andina utilizando diferentes modelos de propagación y herramientas de planificación RF. Proyecto patrocinado por el Fondo Regional para la Innovación Digital en América Latina y el Caribe (FRIDA) y desarrollado por el grupo de Nuevas Tecnologías en Telecomunicaciones (GNTT) de Unicauca con el objetivo de incrementar la inclusión digital en poblaciones del área andina.

---

## **EDUCACIÓN Y ENTRENAMIENTO**

### **Universidad de Murcia**

Doctor en Informática (Seguridad en Servicios y Aplicaciones en Redes), 2011 - 2015

Calificación: Sobresaliente Cum Laude

### **Universidad de Murcia**

Master en Nuevas Tecnologías en Informática (Redes y Telemática), 2010 - 2011

### **Universidad del Cauca**

Grado de Ingeniero, Ingeniería Electrónica y Telecomunicaciones, 2003 - 2009

---

## **CERTIFICACIONES**

### **Certified Ethical Hacker (CEH) V 7.0**

EC-Council. Licencia ECC977492. Abril de 2013

### **Lead Auditor ISO27001 - Information Security Management System (ISMS)**

SGS. Licencia 513410/F/3895. Marzo de 2014

### **Internal Auditor ISO22301 - Business Continuity Management Systems (BCMS)**

SGS. Licencia 39680853/128103886. Julio de 2014

### **ITIL Foundation**

EXIN your ICT competence partner. Licencia 4955987.20238281. Mayo de 2013

---

## **RECONOCIMIENTOS**

Mención: **Doctor internacional. Calificación: Sobresaliente Cum Laude**

Otorgado por: Universidad de Murcia.

Fecha: Noviembre de 2015.

Mención: **Mención de honor en tecnologías de comunicaciones y redes inalámbricas**

Otorgado por: Universidad de Murcia.

Fecha: Junio de 2011.

Mención: **Mención de honor en redes inalámbricas**

Otorgado por: Universidad de Murcia.

Fecha: Junio de 2011

Mención: **Beca de Master**

Otorgado por: Fundación Carolina - Gobierno Español

Fecha: Junio of 2010

Mención: **Media matrícula de honor por alto desempeño académico**

Otorgado por: Universidad del Cauca.

Ocasión: Segundo mejor promedio académico en semestres II-2007, I-2006.

Mención: **Matrícula de honor por alto desempeño académico**

Otorgado por: Universidad del Cauca.

Ocasión: Mejor promedio académico en semestres I-2007, II-2006, II-2005, I-2005.

---

## **PUBICACIONES CIENTIFICAS RELACIONADAS CON SEGURIDAD DE LA INFORMACION**

- Daniel Díaz López, Ginés Dólera Tormo, Félix Gómez Mármol, Gregorio Martínez Pérez, "[Managing XACML systems in distributed environments through Meta-Policies](#)", Computers & Security, vol. 48, pp. 92-115, February 2015 [IF=1.172, Q2 (2013)]
- Daniel Díaz López, Ginés Dólera Tormo, Félix Gómez Mármol, Gregorio Martínez Pérez, "[Dynamic counter-measures for risk-based access control systems: an evolutive approach](#)", Elsevier Future Generation Computer Systems, Special Issue on Trust, Security and Privacy in Distributed Systems, vol. 55, pp. 321-335, 2016 [IF=2.639, Q1 (2013)]
- Daniel O. Díaz López, Ginés Dólera Tormo, Félix Gómez Mármol, José M. Alcaraz Calero, Gregorio Martínez Pérez, "[Live digital, remember digital: State of the art and research challenges](#)", Computers & Electrical Engineering, 40th-year Commemorative Special Issue, vol. 40, no. 1, pp. 109-120, 2014 [IF=0.992, Q3 (2013)]
- D. Díaz López, "[Evaluation of Mobility Proposals with Protocols MIP/SIP in an IMS environment \(IP Multimedia Subsystem\)](#)". Master Thesis, School of Computer Science, June 2011, University of Murcia.
- D. Díaz López, B. Mesa, "[Radio Planning Software Tool for Fixed Wireless Access systems in rural environments](#)". Informatics Technology Management (GTI) Magazine, Industrial University of Santander, issue 8, number 20, 2009.
- D. Díaz López, B. Mesa, "[Radio Planning Software Tool for Fixed Wireless Access systems in rural environments](#)". Diploma Thesis, School of Electronic and Telecommunication Engineering, March 2009, University of Cauca.

---

## **PRODUCCIÓN TECNICA - CONSULTORÍA TECNOLÓGICA Y CIENTÍFICA**

- HUGO FERNEY ÁLVAREZ LUCENA - MARIA ALEJANDRA BLANCO URIBE, DANIEL ORLANDO DIAZ LOPEZ, **Offensive Web Testing Framework (OWTF)**, Conferencia OWASP Latam Tour, Abril 2017, Bogota, Colombia.
- JUAN PABLO ARÉVALO MERCHÁN, ANDRÉS FELIPE VEGA TORRES, DANIEL ORLANDO DIAZ LOPEZ, **OWASP Mobile Project and Internet of Things**, Conferencia OWASP Latam Tour, Abril 2017, Bogota, Colombia.
- TATIANA ANDREA HIGUERA MUNEVAR, NICOLAS MORENO GUATAQUIRA, DANIEL ORLANDO DIAZ LOPEZ, **OWASP SeraphimDroid Project**, Conferencia OWASP Latam Tour, Abril 2017, Bogota, Colombia.
- DAVID ESTEBAN USECHE PELÁEZ, MARIA PAULA BUENO MARTINEZ, DANIEL ORLANDO DIAZ LOPEZ, **The OWASP Enterprise Security API (ESAPI): Security Control Library**, Conferencia OWASP Latam Tour, Abril 2017, Bogota, Colombia.
- DANIEL ORLANDO DIAZ LOPEZ, **Revisión del estado de seguridad de la Información de la Oficina de Tecnología e Informática de la SIC**, contrato/registro: CONTRATO DE PRESTACION DE SERVICIOS No. 799 de 2016 entre la Superintendencia de Industria y Comercio – SIC y DANIEL ORLANDO DIAZ LOPEZ.
- DANIEL ORLANDO DIAZ LOPEZ, **Plan de seguridad de la Oficina de Tecnología e Informática de la SIC**, contrato/registro: CONTRATO DE PRESTACION DE SERVICIOS No. 799 de 2016 entre la Superintendencia de Industria y Comercio – SIC y DANIEL ORLANDO DIAZ LOPEZ.

- DANIEL ORLANDO DIAZ LOPEZ, **Informe de ejecución de campañas de concientización y capacitación en el SGSI**, contrato/registro: CONTRATO DE PRESTACION DE SERVICIOS No. 799 de 2016 entre la Superintendencia de Industria y Comercio – SIC y DANIEL ORLANDO DIAZ LOPEZ.
- DANIEL ORLANDO DIAZ LOPEZ, **Informe de la actualización de la herramienta de apoyo al Sistema de Gestión de Seguridad de la Información (AGGIL)**, contrato/registro: CONTRATO DE PRESTACION DE SERVICIOS No. 799 de 2016 entre la Superintendencia de Industria y Comercio – SIC y DANIEL ORLANDO DIAZ LOPEZ.
- DANIEL ORLANDO DIAZ LOPEZ, **Informe de implementación de controles de seguridad del SGSI (26 controles de seguridad)**, contrato/registro: CONTRATO DE PRESTACION DE SERVICIOS No. 799 de 2016 entre la Superintendencia de Industria y Comercio – SIC y DANIEL ORLANDO DIAZ LOPEZ.
- DANIEL ORLANDO DIAZ LOPEZ, **Plan Estratégico de las Tecnologías de la Información y las Comunicaciones (PETIC) de la SSF**, contrato/registro: CONTRATO INTERADMINISTRATIVO No. 081 de 2015 entre la Superintendencia del Subsidio Familiar - SSF y el Centro de Investigación y Desarrollo en TICs - CINTEL.
- DANIEL ORLANDO DIAZ LOPEZ, **Arquitecturas de TI para la Construcción del PETIC para la SSF**, contrato/registro: CONTRATO INTERADMINISTRATIVO No. 081 de 2015 entre la Superintendencia del Subsidio Familiar - SSF y el Centro de Investigación y Desarrollo en TICs - CINTEL.
- DANIEL ORLANDO DIAZ LOPEZ, **Diagnóstico y Evaluación Tecnológica de la SSF**, contrato/registro: CONTRATO INTERADMINISTRATIVO No. 081 de 2015 entre la Superintendencia del Subsidio Familiar – SSF y el Centro de Investigación y Desarrollo en Tecnologías de la Información y las Comunicaciones – CINTEL.
- DANIEL ORLANDO DIAZ LOPEZ, **Plan de implantación de los controles definidos en la primera fase del PGSI de la SSF**, contrato/registro: CONTRATO INTERADMINISTRATIVO No. 046 de 2015 entre la Superintendencia del Subsidio Familiar – SSF y el Centro de Investigación y Desarrollo en Tecnologías de la Información y las Comunicaciones – CINTEL.
- DANIEL ORLANDO DIAZ LOPEZ, **Manual de políticas y procedimientos de seguridad de la información**, contrato/registro: CONTRATO INTERADMINISTRATIVO No. 195 de 2015 entre la Unidad de Planificación Rural Agropecuaria – UPRA y el Centro de Investigación y Desarrollo en Tecnologías de la Información y las Comunicaciones – CINTEL.
- DANIEL ORLANDO DIAZ LOPEZ, **Metodología de gestión de riesgos de seguridad de la información**, contrato/registro: CONTRATO INTERADMINISTRATIVO No. 195 de 2015 entre la Unidad de Planificación Rural Agropecuaria - UPRA y el Centro de Investigación y Desarrollo en TICs - CINTEL.
- DANIEL ORLANDO DIAZ LOPEZ, **Informe de Ethical Hacking**, contrato/registro: CONTRATO INTERADMINISTRATIVO No. 195 de 2015 entre la Unidad de Planificación Rural Agropecuaria – UPRA y el Centro de Investigación y Desarrollo en Tecnologías de la Información y las Comunicaciones – CINTEL.
- DANIEL ORLANDO DIAZ LOPEZ, **Plan de Tratamiento de Riesgos**, contrato/registro: CONTRATO INTERADMINISTRATIVO No. 453 de 2014 entre la Superintendencia de Industria y Comercio - SIC y el Centro de Investigación y Desarrollo en TICs- CINTEL.
- DANIEL ORLANDO DIAZ LOPEZ, **Definición y/o implementación del modelo de seguridad de la información en las entidades a acompañar**, contrato/registro: CONVENIO INTERADMINISTRATIVO No. 671 DE 2013 suscrito entre el Ministerio de Tecnologías de la Información y el Centro de Investigación y Desarrollo en TICs - CINTEL.

Una lista completa de 47 publicaciones de tipo consultoría tecnológica y científica puede encontrarse en el siguiente link: <http://webs.um.es/felixgm/pubs/managing-access-control-systems-in-distributed-environments-with-dynamic-asset-protection/>