curriculum vitae | CARLOS I. TAPIA

Fecha de nacimiento: 14/05/1981

Estado civil: Soltero, sin hijos

E-mail personal: carlosignaciotapia@gmail.com

Celular: +549-351-8108606

LinkedIn: http://www.linkedin.com/in/carlosignaciotapia

CISA CISSP CEH MASTER

Mi perfil:

Busco continuar mi desarrollo profesional aplicando mi experiencia como Líder de Ciberseguridad Defensiva y Ofensiva, gestionando equipos de trabajo motivados para el éxito de los procesos y proyectos.

EXPERIENCIA LABORAL:

Empresa: Insside (https://www.insside.net)

INSSIDE

Período: Junio 2023 a Junio 2024 (1 año).

Cargo: Blue & Red Team Manager

Personal a cargo: 15 Blue Team; 8 Red Team; 5 IDM

Clientes: Banca, Fintech, Medios de pagos, Retail, laboratorios, utilities

Responsabilidades principales:

- **Red Team**
  - Control de calidad de procesos, documentación y entregables para los servicios:
    - Penetration Testing Web
    - Penetration Testing API
    - Penetration Testing Mobile
    - Penetration Testing de Infraestructura
    - Penetration Testing de ATM/PoS
    - Penetration Testing de Active Directory
    - Penetration Testing de WiFi
    - Penetration Testing Físico
    - Penetration Testing OT (Operational Technology)
    - Servicio de Red Team/Simulación de adversario
    - Simulación de phishing
  - Evaluación de servicios de valor agregado (ejemplo, Servicio de Purple Team, asesoramiento DevSecOps).
  - Dictado de cursos y capacitaciones.
  - Organización del equipo, asignaciones, control de ejecuciones.
  - Planificación de certificaciones profesionales del equipo.
  - Dimensionamientos, evaluación de nuevos clientes y propuestas comerciales/RFP.
  - Reporting interno y externo para auditorías y compliance.

  Tools: Burp Suite, OWASP ZAP, Nikto, Nmap, Iframe Test Online, Postman, MobSF, Nmap, Nessus, Metasploit, Wireshark, Hydra, BloodHound, Mimikatz, CrackMapExec (CME), PowerShell Empire, Wireshark, Aircrack-ng, Kismet, Nexpose, Nikto, Acunetix, etc.

- **Blue Team**
  - Supervisión de procesos de CyberSOC, armado de niveles de atención.
  - Proceso de control de calidad y maduración de CyberSOC/SIEM/SOAR.
  - Proceso de auditoria de SOC-2.
  - Evaluación de capacity.
  - Evaluación de nuevos clientes y propuestas comerciales/RFP.

- **IDM Team**
  - Supervisión de equipo y casos escalados.

- Evaluación de capacity.

Empresa: AMX Argentina S.A. (Claro Argentina, https://www.claro.com.ar)

Período: Abril 2016 a Junio 2023 (7 años y 2 meses).

Cargo: Jefe de Protección de Infraestructura Tecnológica

Personal a cargo: 7 colaboradores en forma directa

Responsabilidades principales:

- **Monitoreo de Ciberseguridad**
  - Supervisión de procesos de CyberSOC, armado de niveles de atención.
  - Armado de playbooks de incidentes y respuesta de mitigación de amenazas.
  - Evaluación e implementación ágil de IoCs (Indicators of Compromise).
  - Revisión de piezas de ciberinteligencia y gestión de contramedidas.
  - Implementación, gestión y madurez de SIEM/SOAR corporativo (IBM Qradar/Resilient).
  - Proceso de control de calidad y maduración de CyberSOC.
  - Reporting interno y externo para auditorías y compliance.
- **Controles preventivos de Ciberseguridad**
  - Gestión de plataformas para la ciberhigiene:
    - Anti-DDoS (Arbor Peakflow).
    - Anti-malware, threat intelligence, EDR para endpoints.
    - Anti-malware para proxy web.
    - Firewalls, IDS/IPS, anti-bot, sandboxing.
    - VPN.
    - Microsoft AD, WSUS, System Center.
    - Consolas de Azure Active Directory, Identity Protection, Cloud App Security (CASB).
    - Colaboración en definición de políticas de Web Application Firewall (F5).
  - Administración y control de parches de Seguridad de Sistemas Operativos y aplicaciones.
  - Gestión de controles de Billetera Virtual (ClaroPay).
  - Administración y explotación del scanner de vulnerabilidades corporativo (Tenable Nessus).
  - Evaluación de procesos de DevSecOps de proveedores de software telco.
  - Configuración y explotación de scanner cloud con herramientas open-source.
  - Solicitudes de scans mediante el scanner corporativo de capa aplicación (Acunetix/Tenable Nessus).
  - Evaluación de riesgos de Seguridad, revisión de controles y hardening de múltiples plataformas de red corporativa, de datacenter y de servicios.
  - Definición y mantenimiento de estrategia y herramientas de Ciberseguridad. Alineación con estrategia del Grupo América Móvil.
  - Gestión de reglas de firewalls, circuito de aprobación y proceso de conciliación de reglas, en cumplimiento con normas Sarbanes-Oxley (Skybox).
  - Implementación de plataforma segura de conexión remota para proveedores (BeyondTrust PasswordSafe).
  - Colaboración en políticas de antispam y protocolos de seguridad de e-mails (SPF, DKIM, DMARC).
  - Evaluación e implementación de controles de Microsoft Office365 (Cloud).
  - Evaluación de riesgos y controles de plataformas Cloud Computing.
  - Evaluación de riesgos y controles de virtualización (VMWare y OpenStack).
  - Participación de proyectos de migración de VPN Corporativa, Zero Trust, SASE, Risk-based Access Control.
  - Evaluación de soluciones antimalware de nueva generación (Crowdstrike, Cylance, Microsoft Defender).
  - Análisis de ataques de Microsoft Active Directory y evaluación de "Firewalls de Active Directory".
  - Evaluación de tecnologías de honeypot (TrapX, Attivo).

- Gestión de proveedores, soporte y licenciamiento de herramientas de seguridad.

- **Otras responsabilidades de gestión**
  - Participación en Comités inter-Gerencias e inter-Direcciones.
  - Atención a Auditoría Interna y Externa por procesos de la Jefatura.
  - Generación y mantenimiento del marco normativo de la Jefatura.
  - Dictado de concientizaciones de Seguridad Informática a otras áreas.

Empresa: Capazeta (https://www.capazeta.com/)

Período: Enero 2015 al presente.

Cargo: Consultor Senior

Responsabilidades principales:

- 01/02/15 – 09/04/15: A cargo de la Auditoría Externa de Sistemas de Sanatorio Allende S.A., relevando los distintos procesos de la Gerencia de Sistemas, informando observaciones de los Controles Generales de IT (con foco en Seguridad Informática) y proponiendo las medidas correctivas pertinentes.
- 04/05/17 – 01/12/17: A cargo de la Auditoría Externa de Sistemas de FAdeA - Fábrica Argentina de Aviones "Brig. San Martín" S. A.
- 01/06/17 – 15/07/17: A cargo de la Auditoría Externa de Sistemas de Box Custodia de Archivos S. A.
- Trainer de cursos basados en CISSP (Certified Information Systems Security Professional), CEH (Certified Ethical Hacker) y normas ISO 27000: cursos a medida para empresas.
- 2021: Auditorías de seguridad para I.S.E.P. (Min. Educación, Prov. De Córdoba), Stoller Argentina S.A. y Graff3D.

Empresa: Hackerone (como Bug Hunter)

Período: Junio 2020 a Enero 2022

Handle: charlywallx

Tareas: Recon, armado de arquitectura y automatización, evaluación de vulnerabilidades de webapp.

Empresa: Grupo Eling S.A. (Grupo Electroingeniería)

Período: Julio 2011 a Abril 2016 (4 años y 9 meses).

Cargo: Responsable de Auditoría Interna de Sistemas

Responsabilidades principales:

- Asistencia en confección y seguimiento de Plan Estratégico de Sistemas.
- Análisis y revisión de políticas y procedimientos referidos a las actividades de Tecnología y Sistemas de Información (mantenimiento y desarrollo de sistemas, ABM de usuarios, operaciones de respaldo y restauración, Disaster Recovery Plan, generación y revisión de logs, gestión de activos de software y hardware, Seguridad Lógica y Física, controles específicos de datacenters, etc.).
- Colaboración en la redacción de políticas, procedimientos y estándares.
- Asistencia en la evaluación de nuevos proyectos de IT, contratos y SLA.
- Revisiones de seguridad del ERP SAP.

- Revisiones de seguridad de Sistemas Operativos Red Hat Enterprise Linux, Debian, Ubuntu y Microsoft Windows XP/2003/7/2008.
- Revisión de configuraciones de seguridad de Bases de Datos MaxDB, MySQL y Microsoft SQL Server.
- Revisión de diseño y seguridad de SAP BI (Data Warehouse).
- Análisis y revisiones de diseño y configuración de redes corporativas, interconexiones entre sedes, obras y oficinas, firewall, IDS, Network Attached Systems, Proxy Web, Samba, Terminal Services, remote administration, etc.
- Revisión y asistencia en la implementación de servicios de directorio LDAP y políticas de grupo en dominios.
- Análisis de la gestión e inventario de activos de tecnología.
- Ejecución de pruebas de Ethical Hacking sobre SAP ERP, aplicaciones web desarrolladas con el framework GeneXus, bases de datos, Content Management Systems Joomla y Alfresco, SugarCRM, Mantis, Maximo Asset Management, OCS Inventory, gestor de cursos Moodle, herramienta colaborativa OpenProject, sistemas operativos versiones clientes y servidores, file servers, e-mail servers, infraestructura de networking, VoIP, wireless LAN, printer attacks, pentest externo de tipo blackbox, greybox y whitebox.
- Revisiones de diseño y controles de Seguridad Física de data centers, salas de cableados y puestos de trabajo.
- Relevamientos del estado de Controles Generales de IT en obras y oficinas de Uniones Transitorias de Empresas (UTE).
- Definición y documentación de Controles Generales de IT.
- Generación, presentación y discusión de Informes de Auditoría Interna de Sistemas dirigidos al Directorio del Grupo.
- Capacitaciones internas sobre Seguridad de Información.
- Montaje y puesta en marcha de servidor de Análisis de Datos mediante software ACL para manipular gran cantidad de registros y efectuar pruebas para el equipo de Auditoría Interna.
- Generación de scripts para la automatización de procesos en ACL Software.
- Monitoreo y seguimiento de upgrade de SAP ERP.
- Monitoreo de performance y Seguridad de la arquitectura SAP ERP.
- Análisis y revisión de políticas y procedimientos operaciones de respaldo y restauración, Disaster Recovery Plan.
- Controles de Seguridad Lógica sobre Sistemas Operativos y Bases de datos de la arquitectura de SAP.
- Planificación cambios de infraestructura de servidores.
- Documentación las órdenes de trabajo y los planes asociados.
- Actualización de normas y procedimientos para adecuarlas a ISO 27001.
- Creación de check-list para controles diarios.
- Gestión a través del sistema de activos y bóveda de contraseñas.
- Dimensionamiento de la estructura de redes necesarias.

Empresa: Ernst & Young (Pistrelli, Henry Martin y Asociados S.R.L.)

Período: Octubre 2003 a Mayo 2011 (7 años y 8 meses)

Cargo: Auditor de Sistemas Senior

Responsabilidades principales:

- Asistencia en la elaboración de Planes Estratégicos de Sistemas alineados a los procesos críticos de negocio.
- Análisis y revisión de políticas y procedimientos referidos a Tecnología y Sistemas de Información (modificación a las aplicaciones, ABM de usuarios, operaciones de respaldo y restauración, Disaster Recovery Plan, generación y revisión de logs, etc.).
- Revisión de configuraciones y definición de estándares de seguridad para Sistemas Operativos Microsoft Windows NT/2000/XP/2003/7/2008.
- Revisión de configuraciones y definición de estándares de seguridad para Sistemas Operativos Unix y Linux.

- Revisión de configuraciones de seguridad para el Sistema Operativo OS/400.
- Revisión de configuraciones de seguridad de Bases de Datos Oracle, Microsoft SQL Server, Informix y Adabas, con sus correspondientes sistemas de Data Warehouse (Business Intelligence).
- Análisis y revisiones de diseño y configuración de redes corporativas, interconexiones entre casas centrales y sucursales, firewall, IDS, etc.
- Revisiones de seguridad del ERP SAP y Oracle Financials.
- Revisiones de controles de seguridad física.
- Definición y documentación de Controles Generales de IT, según metodología EY/GAM (Ernst & Young Global Audit Methodology).
- Documentación de auditorías utilizando software propietario de Ernst & Young (EY/AWS y GAMx).
- Generación, presentación y discusión de Cartas de Comentarios a las Gerencias de las Compañías auditadas.
- Auditorías Internas siguiendo instrucciones de casas matrices.
- Conocimientos de auditoría bajo Ley Sarbanes Oxley Act (SOX).
- Participación en trabajos de hacking ético (test de vulnerabilidades).
- Administración de equipos de trabajos, planificación de compromisos, presupuestación y relevamientos en potenciales clientes.
- Presentaciones para solicitar autorización para llevar los registros contables por medios mecánicos o medios ópticos, ante la Inspección de General de Justicia de CABA y para la Dirección de Inspección de Personas Jurídicas de la Provincia de Córdoba.
- Actividades de comercialización, definición de targets comerciales, mailing promocional y reuniones de presentación de productos de EY – IT Risk & Assurance.
- Actividades de difusión y recruiting de EY en universidades.

FORMACIÓN ACADÉMICA:

Estudios Universitarios:

Carrera:	***Ingeniería de Sistemas***
Entidad:	Instituto Universitario Aeronáutico
Título:	Ingeniero de Sistemas
Nivel:	Grado
Estado:	Egresado
Fecha de obtención:	Diciembre 2012

Carrera:	***Especialización en Seguridad Informática***
Entidad:	Instituto Universitario Aeronáutico
Título:	Especialista en Seguridad Informática
Nivel:	Post-grado
Estado:	Egresado
Fecha de obtención:	Diciembre 2014

Carrera:	***Maestría en Admin. de Negocios (MBA)***
Entidad:	Universidad Empresarial Siglo 21
Título:	Master en Admin. de Negocios (MBA)
Nivel:	Maestría
Estado:	Egresado
Fecha de obtención:	Noviembre 2021

CERTIFICACIONES Y CURSOS TOMADOS:

- **eLearnSecurity Certified Professional Penetration Tester (eCPPTv2)**: en curso.
- Certificado **CEH Master - Certified Ethical Hacker Master** - EC-Council. Certification Number: ECC7526031948.
  - Certificado **CEH - Certified Ethical Hacker** - EC-Council. Certification Number: ECC4518920673.
  - Certificado **CEH Practical - Certified Ethical Hacker Practical** - EC-Council. Certification Number: ECC5843602179.
- Certificación internacional **CISSP (Certified Information Systems Security Professional)**, aprobada en Julio 2022. Licencia (ISC)² ID: **493324**.
- Certificación internacional **CISA (Certified Information Systems Auditor)**, Licencia **13106523**, extendida por ISACA (Information Systems Audit and Control Association) con renovación al día.
- Certificaciones **Microsoft Azure** aprobadas:
  - Microsoft Certified: Azure Fundamentals AZ-900.
  - Microsoft Certified: Azure Security Engineer Associate AZ-500.
  - Microsoft Certified: Security, Compliance, and Identity Fundamentals SC-900.
  - Microsoft Certified Systems Administrator MCSA Win2000/2003.

  Transcript: **https://docs.microsoft.com/en-us/users/carlositapia-5443/transcript/7ollyu428j05304**
- Certificación internacional **CCNA** (Cisco Certified Network Associate), extendida por Cisco Systems. Como preparación para la certificación, se cursaron los 4 semestres del CCNA en Cisco Academy, Universidad Tecnológica Nacional, Facultad Regional Córdoba.
- Training de Ekoparty2018 "**Threat Intelligence vía Malware Analysis**"
- Arbor Networks, cursos de capacitación de plataformas **anti-DDoS**:
  - Peakflow® SP and TMS: DDoS Detection and Mitigation.
  - Peakflow® SP: System Administrator.
  - Peakflow® SP Traffic Analysis/Reporting: Network Monitoring and Traffic Engineering.
- Aprobación del curso "**Administración de Linux a fondo**" (Universidad Tecnológica Nacional, Facultad Regional Córdoba). Carga horaria: 175 hs.
- Diplomatura de "**Seguridad Informática y Hacking de Sistemas**", Universidad Empresarial Siglo 21. Carga horaria: 240 hs.
- Training de Ekoparty2012 Curso dictado por Onapsis "**SAP Security In-Depth**" (pentesting de sistemas SAP).
- Curso Ernst & Young "**SAP IT General Controls**".
- Curso Ernst & Young "**SAP – Cierre de EECC**".
- Curso Ernst & Young "**Windows Active Directory Assessment Essentials**".
- Curso Ernst & Young "**TSRS Skills 500 – Encargado experimentado**".
- Curso Ernst & Young "**ERP Foundation: SAP Financial Statement Close**".
- Curso Ernst & Young "**ERP Foundation: SAP Purchase to Pay**".
- Curso Ernst & Young "**ERP Foundation: SAP Order to Cash**".
- Curso IRAM "**TI-01 La norma IRAM-ISO/IEC 27002. Código de Práctica para la Gestión de Seguridad de la Información**".
- Curso IRAM "**TI-02 La norma IRAM-ISO/IEC 27001. Requisitos para los Sistemas de Gestión de Seguridad de la Información**".

- 22-26/06/15: Seminario "**Cyberwar Bootcamp**" a cargo de Base4 Security y el Coronel Juan José Benítez (Jefe del Centro de Ciberdefensa del Ejército Argentino). Carga horaria: 12 horas.

OTROS ANTECEDENTES:

Área de Tecnología, Auditoría y Seguridad:

- Participación en numerosas Ekoparty Security Conference, Segurinfo (Congreso Iberoamericano de Seguridad de la Información), Encuentro Nacional de Seguridad de la Información & Ciberseguridad, F5 Days y en la conferencia MPOWER Cybersecurity Summit de McAfee en Las Vegas, Nevada, EEUU (Octubre 2017). RSA Security Conference 2020 en San Francisco, California, EEUU (Febrero 2020).
- Conocimientos aplicados de COBIT 5, ISO 27000:2013, ITIL, PMBOK, CMMI, normas diseño de datacenters como ISO/IEC 24764, normas de Seguridad Física como los estándares BICSI, entre otros.
- Numerosos cursos y workshops de seguridad informática, test de vulnerabilidad y temas varios de tecnología.

Área de Ciencias Económicas / Auditoría:

- Febrero 1999 – Diciembre 2002: 3 años aprobados de la carrera de Licenciado en Administración en la Universidad Nacional de Córdoba, Facultad de Ciencias Económicas.
- Cursos internos de metodología Global Audit Methogology de Ernst & Young para Asistente, Asistente Experimentado y Encargado.

Otras Áreas:

- Curso de "Curso Competencias Interpersonales para la gestión de proyectos 2018" (Kinetic).
- "Clínicas de Comunicación para Jefes" 2018 (Claro Argentina).
- Formación en "Gestión de Proyectos" 2017 (Universidad Siglo21).
- Curso de "Oratoria y protocolo" (Universidad Tecnológica Nacional, Facultad Regional Córdoba).
- Curso de "Marketing y técnicas de ventas" (Universidad Tecnológica Nacional, Facultad Regional Córdoba).

Matrícula Profesional:

Matriculado en el Consejo Profesional de Ciencias Informáticas de la Provincia de Córdoba - Matrícula 3108.

ACTUACIÓN DOCENTE:

Instituto Universitario Aeronáutico – Facultad de Ingeniería (Argentina)

- 01/03/15-presente: Nivel de Posgrado - Profesor de la materia **"Auditoría y Control de Seguridad Informática"** de la Especialización en Seguridad Informática.
- 01/06/15-presente: Nivel de Grado – Profesor de la materia "**Auditoría**" de la carrera de Ingeniería en Informática.
- Junio 2016 – presente: tutor de tesis de grado de Ingeniería Informática – IUA (Tesistas: Sánchez, Brizuela-Niro, Alasia-Polanco, Irigoitía, Meléndez).

- Diciembre 2016-presente: tutor de tesis de posgrado de Especialista en Seguridad Informática (Tesistas: Coenda, Colmenarez, Vega, Sarchetti, Melendez).

Universidad Nacional de Córdoba – FaMAF (Argentina)

- Enero 2016: miembro de tribunal evaluador de tesis de posgrado de la Especialización en Criminalística y Actividades Periciales - Universidad Nacional de Córdoba – FaMAF.

Universidad Católica de Córdoba – Facultad de Ingeniería (Argentina)

- Junio 2022-presente: asesor de tesis de grado (Tesista: Reznichenco).

Universidad Empresarial Siglo 21 (Argentina):

- 01/04/23-presente: Nivel de Posgrado - Profesor de la materia **"Seguridad Ofensiva"** de la Especialización en Cibercrimen.

Universidad Autónoma de Encarnación – UNAE (Paraguay):

- Mayo-Junio 2023: Nivel de Posgrado - Profesor de la materia **"Seguridad en Sistemas Operativos y Aplicaciones I"** de la Especialización en Seguridad Informática.
- Julio-Agosto 2023: Nivel de Posgrado - Profesor de la materia **"Seguridad en Sistemas Operativos y Aplicaciones II"** de la Especialización en Seguridad Informática.
- Septiembre-Noviembre 2023: Nivel de Posgrado - Profesor de la materia **"Trabajo Final Integrador"** de la Especialización en Seguridad Informática.

Intertron S.A. - Intertron Education:

- A cargo del curso "**Gestión de Seguridad de la Información**" (dictado en forma regular desde 2015 a la fecha).
  - Módulo 01 - Arquitecturas y modelos de Seguridad
  - Módulo 02 - Sistemas y métodos de control de acceso
  - Módulo 03 - Seguridad de Operaciones
  - Módulo 04 - Criptografía
  - Módulo 05 - Seguridad Física
  - Módulo 06 - Recuperación ante desastres
  - Módulo 07 - Seguridad en Internet, redes y telecomunicaciones
  - Módulo 08 - Legislación y Compliance
  - Módulo 09 - Informática Forense
  - Módulo 10 - Cibercrimen y hacktivismo
  - Módulo 11 - Evaluaciones de seguridad
  - Módulo 12 - Ethical Hacking
  - Módulo 13 - Seguridad en desarrollo
  - Módulo 14 - Tratamiento malware
  - Módulo 15 - Respuesta incidentes
- A cargo del módulo de Seguridad y hardening del Curso "**20411: Administering Windows Server 2012**" (dictado en 2015).
- A cargo del módulo de Seguridad y hardening del Curso "**10775A - Administering Microsoft SQL Server 2012 Databases**" (dictado en 2015).

EducaciónIT:

A cargo de los siguientes cursos durante 2017:

- Introducción a la Seguridad Informática.
- Seguridad en Redes: Network Hacking
- Introducción a Redes.

INVESTIGACIÓN Y PUBLICACIONES:

Papers presentados y aprobados:

- 21/11/13 - Trabajo de investigación aprobado y expuesto "**Honeynets como herramienta de prevención e investigación de ciberataques**", 1er Congreso Nacional de Ingeniería Informática / Sistemas de Información (CoNaIISI'2013), organizado por CONFEDI (Consejo Federal de Decanos de Ingeniería) en la Facultad Regional Córdoba - Universidad Tecnológica Nacional.
- 08/10/14 - Trabajo de investigación aprobado y expuesto "**Fortalecimiento de la Seguridad de las comunicaciones mediante la implementación de una Infraestructura de Clave Pública**", 6° Jornadas de Ciencia y Tecnología (CyTAL 2014), Secretaria de Ciencia y Tecnología de la Facultad Regional Villa María - Universidad Tecnológica Nacional.
- 06/05/15 - Trabajo de investigación aprobado **"Fortalecimiento en la Seguridad de Web Services para Aplicaciones Críticas"**. 44JAIIO, Jornadas Argentinas de Informática 2015, Rosario.
- 08/02/16 - Trabajo de investigación aprobado "**Implementación de Redes Señuelo como técnica de mejoramiento de la Ciberdefensa**", 7° Jornadas de Ciencia y Tecnología (CyTAL 2016), Secretaria de Ciencia y Tecnología de la Facultad Regional Villa María - Universidad Tecnológica Nacional.
- 09/09/16 - "**Manejo eficiente de eventos de Seguridad de honeynets mediante BigData**", 45 JAIIO, Jornadas Argentinas de Informática, organizado por Universidad Tres de Febrero, sede Centro Cultural Borges - CABA.
- 29-30/11/16 - 2 trabajos de investigación aprobados y presentados en el **ISC² Security Congress Latin America 2016** en San Pablo Brasil. Trabajos:
  - **Efficient Management of Security Logs from Honeynets through Big Data**. Autores: Carlos Ignacio Tapia, Eduardo Casanovas, Fernando Boiero, Mariano Garcia Mattio y Francisco Coenda.
  - **An Approach to Automated Malware Analysis through Online Diagnostic Tools**. Autores: Carlos Ignacio Tapia, Eduardo Casanovas, Tomas Niro y Ruy Brizuela – Argentina
- 02/11/17 - paper aprobado y presentado "**Honeypots Web como Herramientas de Análisis de Ciberataques sobre una Red de Telefonía Móvil**", 5to Congreso Nacional de Ingeniería Informática / Sistemas de Información (CoNaIISI'2017), organizado por CONFEDI (Consejo Federal de Decanos de Ingeniería) en la Facultad Regional Santa Fe - Universidad Tecnológica Nacional.
- 07/09/18 - poster aprobado y presentado "**Identificación de necesidades de monitoreo de ciberseguridad enfocado en el segmento PyMEs**", 47 JAIIO, Jornadas Argentinas de Informática, organizado por Facultad de Ingeniería - Universidad de Palermo - CABA.
- 06/06/19 - paper aprobado y presentado "**Cazadores de ciberamenazas como parte fundamental de un CyberSOC moderno**", 3° Conferencia Nacional de Informática Forense (Info-Conf), Facultad de Ciencias Exactas, Físicas y Naturales – Universidad Nacional de Córdoba.

Disertaciones conducidas:

- 04/09/14 - Exposición de la temática "**Honeynets como herramienta de prevención e investigación de ciberataques**", EduTech14, SemanaTIC14, organizado por el Gobierno de la Provincia de Córdoba.

- 01/04/15 - Presentación **"Utilización de herramientas de Ciberdefensa para aplicar en Infraestructuras Criticas"**. Jornada de Ciberdefensa del Ministerio de Defensa de la Nación en la ciudad de Rafaela, Santa Fe.
- 15/04/15 - Presentación **"Protección de software mediante Firma Digital en el marco de la Ciberdefensa Nacional"**. Jornada de Ciberdefensa del Ministerio de Defensa de la Nación en la ciudad de Ascochinga, Córdoba.
- 04/09/14 - Exposición de la temática "**Seguridad en el manejo y control de datos**", EduTech14, SemanaTIC16, organizado por el Gobierno de la Provincia de Córdoba.

Grupos de investigación:

- 03/03/15 - 30/06/2016: Proyecto de Investigación para la Defensa (PIDDEF) del Ministerio de Defensa de la Nación **"Implementación de sistemas señuelo para prevención e investigación de ciberataques en el marco de la Ciberdefensa Nacional"**. Cargo: Coordinador General de Proyecto. Responsabilidades: coordinación de equipos, definición de objetivos, definición de herramientas, generación de documentación. Grupo de trabajo: 11 personas.
- 23/11/15 - presente: Co-líder del **Chapter Argentina** del Honeynet Project.

IDIOMAS:

- Español (lengua materna).
- Inglés (EF SET C2 Proficient).