



JUAN DIEGO CAMPO  
BARBÉ

Dr. Ing.

[jdcampo@fing.edu.uy](mailto:jdcampo@fing.edu.uy)

Julio Herrera y Reissig 565  
27142714 (12121)

### SNI

Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información

Categorización actual: Iniciación (Activo)

Fecha de publicación: 18/06/2025  
Última actualización: 30/05/2025

## Datos Generales

### INSTITUCIÓN PRINCIPAL

Universidad de la República/ Facultad de Ingeniería / Instituto de Computación / Uruguay

### DIRECCIÓN INSTITUCIONAL

Institución: Universidad de la República / Facultad de Ingeniería / Sector Educación Superior/Público

/ Instituto de Computación

Dirección: Julio Herrera y Reissig 565 / 11300

País: Uruguay / Montevideo / Montevideo

Teléfono: (598) 27142714 / 12121

Correo electrónico/Sitio Web: [jdcampo@fing.edu.uy](mailto:jdcampo@fing.edu.uy)

## Formación

### Formación académica

#### CONCLUIDA

#### DOCTORADO

##### Doctorado en Informática (UDELAR-PEDECIBA) (2013 - 2015)

Universidad de la República - Facultad de Ingeniería , Uruguay

Título de la disertación/tesis/defensa: Formally Verified Countermeasures Against Cache Based Attacks in Virtualization Platforms

Tutor/es: Gilles Barthe, Gustavo Betarte

Obtención del título: 2016

Sitio web de la disertación/tesis/defensa:

[http://www.fing.edu.uy/inco/grupos/gsi/documentos/tesis/thesis\\_jdcampo.pdf](http://www.fing.edu.uy/inco/grupos/gsi/documentos/tesis/thesis_jdcampo.pdf)

Palabras Clave: non-interference cache-based attacks constant-time cryptography stealth memory Coq

Áreas de conocimiento:

Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información / Ingeniería de Sistemas y Comunicaciones / Seguridad Informática

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Métodos Formales

#### GRADO

##### Analista en Computación (2002 - 2005)

Universidad de la República - Facultad de Ingeniería , Uruguay

Título de la disertación/tesis/defensa:

Obtención del título: 2005

Áreas de conocimiento:

Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información / Ingeniería de Sistemas y Comunicaciones /

##### Ingeniería en Computación (2002 - 2009)

Universidad de la República - Facultad de Ingeniería , Uruguay

Título de la disertación/tesis/defensa: Framework for IT Security Training

Tutor/es: Gustavo Betarte, Alejandro Blanco, Marcelo Rodríguez

Obtención del título: 2009

Sitio web de la disertación/tesis/defensa: <https://www.fing.edu.uy/inco/grupos/gsi/thesis/design-development-framework-it-security-training/>

Áreas de conocimiento:

Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información / Ingeniería de Sistemas y Comunicaciones / Seguridad Informática

## Formación complementaria

### CONCLUIDA

#### CURSOS DE CORTA DURACIÓN

##### **Programa Sensibilización en Género, Módulo I - Introducción a la temática de Género (09/2023 - 09/2023)**

Sector Educación Superior/Público / Universidad de la República / Pro Rectorado de Gestión Administrativa / Comisión Abierta de Equidad y Género, Uruguay  
10 horas

##### **Programa Sensibilización en Género, Módulo II - Transversalización de Género en las organizaciones y en la Udelar (09/2023 - 09/2023)**

Sector Educación Superior/Público / Universidad de la República / Pro Rectorado de Gestión Administrativa / Comisión Abierta de Equidad y Género, Uruguay  
10 horas

##### **Introducción a la Didáctica de la Informática (10/2010 - 11/2010)**

Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería / Instituto de Computación, Uruguay

#### PARTICIPACIÓN EN EVENTOS

##### **Oregon Programming Languages Summer School (2011)**

Tipo: Seminario

Institución organizadora: University of Oregon, Estados Unidos

Palabras Clave: Lenguajes de programación Métodos Formales Teoría de Tipos

Áreas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Métodos Formales

## Idiomas

### **Español**

Entiende muy bien / Habla muy bien / Lee muy bien / Escribe muy bien

### **Inglés**

Entiende muy bien / Habla muy bien / Lee muy bien / Escribe muy bien

### **Japonés**

Entiende bien / Habla bien / Lee bien / Escribe bien

## Áreas de actuación

### **INGENIERÍA Y TECNOLOGÍA**

Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información / Ingeniería de Sistemas y Comunicaciones / Seguridad Informática

### **CIENCIAS NATURALES Y EXACTAS**

Ciencias de la Computación e Información / Ciencias de la Computación / Métodos Formales

## Actuación profesional

**SECTOR EDUCACIÓN SUPERIOR/PÚBLICO - UNIVERSIDAD DE LA REPÚBLICA - URUGUAY**

## VÍNCULOS CON LA INSTITUCIÓN

### **Funcionario/Empleado (10/2021 - a la fecha)** Trabajo relevante

30 horas semanales / Dedicación total  
Escalafón: Docente  
Grado: Grado 3  
Cargo: Efectivo

### **Funcionario/Empleado (08/2018 - 09/2021)**

Profesor Adjunto 10 horas semanales  
Escalafón: Docente  
Grado: Grado 3  
Cargo: Efectivo

### **Funcionario/Empleado (07/2011 - 08/2018)**

Asistente 12 horas semanales  
Escalafón: Docente  
Grado: Grado 2  
Cargo: Efectivo

### **Funcionario/Empleado (05/2009 - 07/2011)**

Ayudante 15 horas semanales  
Escalafón: Docente  
Grado: Grado 1  
Cargo: Interino

## ACTIVIDADES

### LÍNEAS DE INVESTIGACIÓN

#### **Seguridad en Dispositivos Móviles (03/2014 - a la fecha )**

Esta línea se centra en investigar y proponer un enfoque integral que permita abordar el problema de gestión de vulnerabilidades de seguridad en plataformas de dispositivos móviles, de manera rigurosa y sistemática, mediante el diseño de mecanismos autónomos certificados capaces de acompañar tecnologías móviles en rápida expansión.

Fundamental

5 horas semanales

Instituto de Computación, Grupo de Seguridad Informática , Integrante del equipo

Equipo: Juan Diego CAMPO BARBÉ , Gustavo BETARTE GUIDI , Carlos Daniel LUNA GARCIA

Áreas de conocimiento:

Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información / Ingeniería de Sistemas y Comunicaciones / Seguridad Informática

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Métodos Formales

#### **Seguridad de Aplicaciones Web (05/2017 - a la fecha )**

Esta línea intenta integrar técnicas de distintas áreas del conocimiento, como ser aprendizaje automático, minería de datos y seguridad guiada por modelos, para la construcción de herramientas capaces de incrementar el nivel de aseguramiento de aplicaciones web. El desarrollo de técnicas de detección de ataque, en particular, involucra procedimientos que ayudan a discernir entre el comportamiento de un usuario válido del sistema y un actor (humano o mecánico) malicioso. La identificación y determinación de un comportamiento no contemplado (anómalo) debe tener en cuenta si cada evento detectado es simplemente sospechoso, o si en realidad se trata de un evento que es parte de un incidente de seguridad, y particularmente de un ataque.

Aplicada

10 horas semanales

Instituto de Computación, Grupo de Seguridad Informática , Integrante del equipo

Equipo: Juan Diego CAMPO BARBÉ

Áreas de conocimiento:

Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información / Ingeniería de Sistemas y Comunicaciones / Seguridad Informática

### **Seguridad en IoT (05/2018 - a la fecha )**

En esta línea de investigación se estudian los problemas de seguridad particulares de las redes de dispositivos IoT. En particular se busca entender y modelar las variadas amenazas presentes en esta nueva tecnología y posibles formas de mitigación de las mismas.

Aplicada

5 horas semanales

Instituto de Computación, Grupo de Seguridad Informática , Integrante del equipo

Equipo: Juan Diego CAMPO BARBÉ , Gustavo BETARTE GUIDI

Areas de conocimiento:

Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información / Ingeniería de Sistemas y Comunicaciones / Seguridad Informática

Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información / Ingeniería de Sistemas y Comunicaciones / Internet de las cosas

### **Seguridad de Contratos inteligentes (05/2018 - a la fecha )**

El objetivo de esta línea de investigación es estudiar la seguridad de plataformas blockchain y en especial estudiar formas de dar garantías de seguridad sobre contratos inteligentes, por medio por ejemplo de la aplicación de métodos formales para razonar sobre su comportamiento.

Mixta

1 horas semanales

Instituto de Computación, Grupo de Seguridad Informática , Integrante del equipo

Equipo: Juan Diego CAMPO BARBÉ , Gustavo BETARTE GUIDI , Carlos Daniel LUNA GARCIA

Areas de conocimiento:

Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información / Ingeniería de Sistemas y Comunicaciones / Seguridad Informática

### **Laboratorios de Seguridad Informática (05/2009 - a la fecha )**

Esta línea de investigación tiene como objetivo general el diseñar, desarrollar e implantar plataformas para el entrenamiento en seguridad informática.

5 horas semanales

Instituto de Computación, Grupo de Seguridad Informática , Integrante del equipo

Equipo: Juan Diego CAMPO BARBÉ

Palabras clave: Seguridad Informática Laboratorios de Seguridad Virtualización

Areas de conocimiento:

Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información / Ingeniería de Sistemas y Comunicaciones /

### **Verificación Formal de Seguridad en plataformas de virtualización (05/2009 - a la fecha )**

Esta línea se enfoca en desarrollar modelos idealizados de sistemas informáticos críticos y construir pruebas matemáticas que muestren que el modelo satisface propiedades de seguridad como no interferencia. Hemos estudiado principalmente plataformas de virtualización, y más específicamente hipervisores, que permiten la coexistencia de distintos sistemas operativos en el mismo hardware. Nuestros modelos nos permiten razonar sobre el aislamiento de los distintos sistemas operativos ejecutando en la plataforma, incluso en presencia de los llamados canales laterales.

8 horas semanales

Instituto de Computación, Grupo de Seguridad Informática , Integrante del equipo

Equipo: Juan Diego CAMPO BARBÉ

Palabras clave: Seguridad Informática

Areas de conocimiento:

Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información / Ingeniería de Sistemas y Comunicaciones / Seguridad Informática

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Métodos Formales

## **PROYECTOS DE INVESTIGACIÓN Y DESARROLLO**

### **Herramientas conceptuales y tecnológicas para ciberseguridad adaptativa y certificada (04/2023 - a la fecha)**

El objetivo de este programa de investigación es el de continuar trabajando en líneas ya exploradas y explorar nuevos aspectos en los siguientes dominios complementarios de investigación: (1) la concepción y desarrollo de mecanismos automatizados de identificación, análisis y prevención de ataques informáticos aplicaciones web y sistemas informáticos basados en técnicas de aprendizaje

automático y profundo, de seguridad guiada por modelos y de minería de procesos, (2) el desarrollo de metodologías y herramientas que permitan montar un Cyber Range que sea una plataforma de avanzada para la formación, entrenamiento, experimentación e investigación en torno a los múltiples aspectos de la ciberseguridad y (3) desarrollar, adaptar y especializar métodos, técnicas y herramientas para la verificación de contratos inteligentes, protocolos y plataformas de cómputo basadas en criptomonedas.

10 horas semanales

Investigación

Coordinador o Responsable

En Marcha

RRHH formados en el proyecto:

Pregrado:1

Maestría/Magister:2

Doctorado:1

Financiación:

Comisión Sectorial de Investigación Científica, Uruguay, Apoyo financiero

Equipo: JUAN DIEGO CAMPO (Responsable), G. BETARTE (Responsable), LUNA, C., Maximiliano CRISTIÁ, A. SILVEIRA, G. Guerrero, M. RODRÍGUEZ, R. MARTÍNEZ, A. Blanco, M. E. Corti, Nicolas Serrano, ALVARO PARDO, María Fernanda MOLINA GIUDICE

#### **ModSecIntl: A machine learning-assisted web application firewall (10/2021 - 10/2022 )**

The general objective of this project is the conception and development of automated mechanisms for the identification, analysis and prevention of computer attacks on web applications. The technological result of the project will be a Minimum Viable Product (MVP) consisting of models and tools that allow automated support to these mechanisms.

10 horas semanales

Investigación

Integrante del Equipo

Concluido

RRHH formados en el proyecto:

Maestría/Magister:1

Financiación:

OEA, Estados Unidos, Apoyo financiero

Equipo: JUAN DIEGO CAMPO, G. BETARTE (Responsable), D. CALEGARI, Nicolás Montes, ALVARO PARDO, R. MARTÍNEZ, M. RODRÍGUEZ, FZIPI, Amanda Riverol, Fernando Outeda  
Palabras clave: ModSecurity Web Application Firewall machine learning deep learning Computer Security

#### **Automatización de derivación de conocimiento para el aseguramiento de sistemas informáticos (05/2018 - 05/2021 )**

Este proyecto se focaliza en la búsqueda de soluciones que incorporen la adaptación de técnicas de aprendizaje automático, minería de datos y seguridad guiada por modelos para la especificación de mecanismos y construcción de herramientas cuya utilización permita incrementar el nivel de aseguramiento de aplicaciones web.

8 horas semanales

Instituto de Computación, Grupo de Seguridad Informática

Investigación

Integrante del Equipo

En Marcha

RRHH formados en el proyecto:

Maestría/Magister:1

Financiación:

Agencia Nacional de Investigación e Innovación, Uruguay, Apoyo financiero

Equipo: JUAN DIEGO CAMPO, G. BETARTE (Responsable), A. PARDO, D. CALEGARI, LUNA, C., M. RODRÍGUEZ, R. MARTÍNEZ, FZIPI, Víctor CODOCEDO

Palabras clave: Aprendizaje automático y minería de datos Seguridad basada en modelos Ciberinteligencia

Áreas de conocimiento:

Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información / Ingeniería de Sistemas y Comunicaciones / Seguridad Informática

#### **Desafíos de seguridad y privacidad en el diseño e implementación de soluciones de rastreo digital de proximidad (05/2020 - 11/2020 )**

La utilidad de una aplicación de rastreo digital de proximidad (RDP) radica en su capacidad para

detectar contactos en riesgo y utilizar esta información en conjunto con otras medidas para combatir la epidemia, como la realización de tests, el distanciamiento social o la cuarentena. En el contexto del proyecto PROTECT se ha trabajado en identificar las propuestas existentes, las tecnologías, flujos de datos y procesos involucrados en el funcionamiento de sistemas RDP. Este proyecto ha sido postulado al llamado del Programa CSIC Conocimiento especializado para enfrentar la emergencia planteada por el COVID19 y sus impactos y ha sido seleccionado para recibir apoyo del programa.

5 horas semanales

Investigación

Integrante del Equipo

En Marcha

Financiación:

Comisión Sectorial de Investigación Científica, Uruguay, Apoyo financiero

Equipo: JUAN DIEGO CAMPO , G. BETARTE , A. DELGADO , P. EZZATTI , A. FORTEZZA , L. GONZALEZ , A. MARTIN , B. MURACCIOLE , R. RUGGIA

Palabras clave: COVID19 rastreo digital de proximidad soluciones tecnológicas protección de datos personales seguridad informática

### **Mecanismos autónomos de seguridad certificados para sistemas computacionales móviles (01/2015 - 01/2018)**

El desarrollo masivo de tecnologías móviles ha cambiado radicalmente la manera en la que los usuarios acceden y utilizan los recursos informáticos disponibles hoy en día. Esta evolución ha generado un aumento considerable en la complejidad de la gestión de estas tecnologías, tanto desde el punto de vista de la infraestructura como de los dispositivos individuales. En este contexto, mecanismos de seguridad capaces de proteger la información y las actividades desarrolladas por el usuario final, así como las de las organizaciones con las que los mismos se interconectan, son fundamentales. Sin embargo, los temas de seguridad han sido usualmente relegados detrás de avances de carácter operacional y funcional. El objetivo principal de este proyecto es investigar y proponer un enfoque integral que permita abordar el problema de gestión de vulnerabilidades de seguridad en plataformas de dispositivos móviles, de manera rigurosa y sistemática, mediante el diseño de mecanismos autónomos certificados capaces de acompañar tecnologías móviles en rápida expansión. Dado su extendido uso como sistema operativo de teléfonos inteligentes (smartphones), en este proyecto se considerará la plataforma Android como dominio objetivo de experimentación y validación de los mecanismos y metodologías que se pretende abordar y desarrollar en este proyecto.

12 horas semanales

Instituto de Computación , Grupo de Seguridad Informática

Investigación

Integrante del Equipo

Concluido

Financiación:

Agencia Nacional de Investigación e Innovación, Uruguay, Apoyo financiero

Equipo: MARCELO RODRÍGUEZ , GUSTAVO BETARTE (Responsable) , CARLOS LUNA , FELIPE ZIPITRÍA , MAXIMILIANO CRISTÍA , MARTÍN BARRERE , Juan Diego CAMPO

### **VirtualCert: Hacia una Plataforma de Virtualización Certificada - Fase II (03/2013 - 12/2014)**

Este proyecto establece líneas de trabajo que han sido identificadas y que ya se han comenzado a explorar en el trabajo de investigación realizado en el proyecto de Investigación Fundamental Fondo Clemente Estable VirtualCert: Hacia una Plataforma Certificada de Virtualización (proyecto FCE2009\_PR\_1\_2568). La primera fase del proyecto fue finalizada en julio de 2012. Como resultado del trabajo de investigación desarrollado en el proyecto VirtualCert, ya se cuenta con una versión completamente formalizada y verificada usando el asistente de pruebas Coq [Coq10, BC04] de un modelo idealizado de una plataforma de virtualización en la que se modelan las diferentes estructuras de memoria que pueden ser gestionadas por los sistemas operativos (SOs) guests de la plataforma. Asimismo, se han establecido y probado propiedades de seguridad que garantizan que los sistemas operativos guests solamente tienen acceso a la memoria que les pertenece, sin poder disturbar la de los otros sistemas con los que comparten los recursos de la plataforma de hardware virtualizada. Estas últimas propiedades han sido formuladas como propiedades de non-interference, o más precisamente, non-influence. El objetivo principal que se ha definido para esta Fase II del proyecto consiste en desarrollar una extensión del modelo con componentes que permitan la formulación de ataques basados en cache y poder probar formalmente que para este tipo de ataques que la plataforma cuenta con mecanismos de seguridad que permiten prevenir eficazmente los mismos. Este tipo de estudios es de alto interés para la comunidad de métodos formales y provable security. Como un primer paso en esa dirección ya se

cuenta con una extensión del modelo que nos permite formular cache-based probing attacks y se ha probado formalmente que para este tipo de ataques, en presencia de una estructura VIVT (Virtually Indexed Virtually Tagged) de cache con una política escritura write-through, la plataforma modelada cuenta con mecanismos de seguridad que permiten prevenir eficazmente los mismos. En el caso de una estructura de cache de tipo VIPT (Virtually Indexed Physically Tagged) el análisis de propiedades de no influencia es de particular interés, ya que el costoso mecanismo de vaciado (flushing) de la cache en un cambio de contexto (empleado por caches de tipo VIVT) no es utilizado, permitiendo que la cache pueda contener en un momento dado páginas de memoria de diferentes sistemas operativos. Por otra parte, analizar no influencia en el contexto de diferentes políticas de escritura de cache permitiría complementar la investigación realizada en la fase anterior del proyecto. La actividad de investigación a desarrollar en la Fase II del proyecto VirtualCert, se focalizará entonces en dos líneas principales de trabajo, a saber: el modelado de estructuras de cache VIPT y las correspondientes pruebas de no influencia y el desarrollo una extensión del modelo que permita establecer y probar formalmente propiedades de seguridad relacionadas con ataques basados en la observación de la gestión de la memoria cache.

8 horas semanales

Instituto de Computación , Grupo de Seguridad Informática

Investigación

Integrante del Equipo

Concluido

RRHH formados en el proyecto:

Pregrado:2

Doctorado:2

Financiación:

Comisión Sectorial de Investigación Científica, Uruguay, Apoyo financiero

Equipo: GUSTAVO BETARTE (Responsable) , CARLOS LUNA , GILLES BARTHE , Juan Diego CAMPO

Palabras clave: Virtualización No interferencia

Areas de conocimiento:

Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información / Ingeniería de Sistemas y Comunicaciones / Seguridad Informática

#### **VirtualCert: Hacia una plataforma de virtualización certificada (01/2010 - 12/2012)**

Este proyecto aborda el estudio del comportamiento de plataformas de computación virtuales. Concretamente, se focaliza en la especificación y verificación formal de determinadas propiedades de seguridad, que es deseable sean garantizadas por plataformas de virtualización sobre las que son ejecutadas variedades de máquinas virtuales que ofician de hosts a sistemas operativos, sean estos confiables o no. En particular, interesa modelar formalmente la interacción de diferentes sistemas operativos ejecutando sobre una misma plataforma virtualizada y establecer cuáles son los mecanismos que garantizan determinadas propiedades de no interferencia, particularmente en relación a los datos manejados por los sistemas que ejecutan concurrentemente sobre esa plataforma.

8 horas semanales

Instituto de Computación , Grupo de Seguridad Informática

Investigación

Integrante del Equipo

Concluido

RRHH formados en el proyecto:

Pregrado:2

Maestría/Magister:1

Financiación:

Agencia Nacional de Investigación e Innovación, Uruguay, Apoyo financiero

Equipo: GUSTAVO BETARTE (Responsable) , CARLOS LUNA , GILLES BARTHE , Juan Diego Campo

Palabras clave: Virtualización

Areas de conocimiento:

Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información / Ingeniería de Sistemas y Comunicaciones / Seguridad Informática

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Métodos Formales

#### **DOCENCIA**

**Ingeniería en Computación (03/2012 - a la fecha)**

Grado  
Asistente  
Asignaturas:  
Lógica, 10 horas, Teórico-Práctico

**Ingeniería en Computación (09/2009 - a la fecha)**

Grado  
Asistente  
Asignaturas:  
Fundamentos de la Seguridad Informática, 10 horas, Práctico  
Áreas de conocimiento:  
Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información / Ingeniería de Sistemas y Comunicaciones / Programación

**Ingeniería en Computación (07/2021 - 11/2021 )**

Grado  
Asistente  
Asignaturas:  
Taller de Introducción a la Computación, 5 horas, Teórico-Práctico

**Centro de Posgrados y Actualización Profesional (05/2011 - 05/2013 )**

Especialización  
Asistente  
Asignaturas:  
Seguridad en Sistemas Operativos, 4 horas, Práctico  
Seguridad en Redes TCP/IP, 4 horas, Práctico  
Áreas de conocimiento:  
Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información / Ingeniería de Sistemas y Comunicaciones / Seguridad Informática

**Ingeniería en Computación (07/2009 - 12/2011 )**

Grado  
Asistente  
Asignaturas:  
Programación 3, 10 horas, Práctico

**Maestría en Informática PEDECIBA (03/2011 - 06/2011 )**

Maestría  
Asistente  
Asignaturas:  
Taller de Recursos de Investigación, 1 hora, Teórico-Práctico

**EXTENSIÓN**

**Participación en talleres con escuelas sobre aerogeneradores (09/2024 - 09/2024 )**

1 hora

**Convenio con AGESIC para la generación de una currícula de formación en ciberseguridad a nivel terciario (06/2022 - 12/2022 )**

5 horas

**CAPACITACIÓN/ENTRENAMIENTOS DICTADOS**

**Taller para instructores de Tectonic para varias universidades latinoamericanas, Red Ciberlac - Red CLARA (11/2024 - a la fecha )**

Taller Train the trainers  
2 horas semanales

**Dictado de taller para instructores de Tectonic, Jornadas Uruguayas de Ciencias de la Computación 2024 (12/2024 - 12/2024)**

Taller TTT Tectonic  
1 hora semanales

**Participación en el dictado del curso "Análisis Forense y respuesta a incidentes", III Escuela Latinoamericana de Informática del CLEI. Agosto 2024, Bahía Blanca, Argentina. (08/2024 - 08/2024)**

Análisis Forense y respuesta a incidentes  
5 horas semanales

**Actividad de entrenamiento en Ciberseguridad (11/2023 - 11/2023)**

Red de Excelencia en Ciberseguridad de Latinoamérica y el Caribe (Ciberlac)  
5 horas semanales

#### **SERVICIO TÉCNICO ESPECIALIZADO**

**Miembro del equipo que realizó el análisis de riesgos de seguridad y privacidad de la aplicación CoronavirusUY (07/2020 - 08/2020 )**

5 horas semanales

#### **PASANTÍAS**

**Pasantía de investigación con el Dr. Gilles Barthe y su equipo en el Instituto Madrileño de Estudios Avanzados (IMDEA Software), Madrid, España (11/2010 - 12/2010 )**

40 horas semanales

#### **OTRA ACTIVIDAD TÉCNICO-CIENTÍFICA RELEVANTE**

**Integración de tribunales de evaluación de proyectos de grado (07/2011 - a la fecha )**

1 horas semanales

**Representante alterno por la Facultad de Ingeniería, Udelar a la Red de Excelencia en Ciberseguridad en Latinoamérica y el Caribe (CiberLac) (10/2021 - a la fecha )**

1 horas semanales

**Participación en tribunal para Llamado a Docente Encargado para el área de Arquitectura, Sistemas Operativos y Redes de Computadoras del Tecnólogo en Informática de San José de la UTEC (03/2023 - 06/2023 )**

1 horas semanales

**Participación en tribunal para dos llamados a Jefe de Informática e Ingenieros de Soporte de la CJPPU (03/2021 - 06/2021 )**

1 horas semanales

**Participación en tribunal de concurso del BROU para cargo de Analista de Seguridad (04/2020 - 07/2020 )**

1 horas semanales

#### **GESTIÓN ACADÉMICA**

**Delegado titular por el orden docente a la ACF (02/2022 - a la fecha )**

Asamblea del Claustro de Facultad Participación en cogobierno 3 horas semanales

**Delegado suplente por el orden docente de la comisión de instituto (05/2023 - a la fecha )**

Instituto de Computación Participación en cogobierno 5 horas semanales

**Delegado suplente por el orden docente de la comisión de instituto (02/2017 - 11/2018 )**

Instituto de Computación, Comisión de Instituto  
Participación en cogobierno 2 horas semanales

#### **SECTOR EDUCACIÓN SUPERIOR/PÚBLICO - PROGRAMA DE DESARROLLO DE LAS CIENCIAS BÁSICAS - URUGUAY**

Área Informática (PEDECIBA)

## VÍNCULOS CON LA INSTITUCIÓN

### **Colaborador (05/2017 - a la fecha)** Trabajo relevante

Investigador grado 3 10 horas semanales

## ACTIVIDADES

### GESTIÓN ACADÉMICA

#### **Miembro del Consejo Científico del Área Informática del PEDECIBA (03/2022 - 02/2024)**

Gestión de la Investigación 2 horas semanales

### SECTOR EDUCACIÓN SUPERIOR/PÚBLICO - UNIVERSIDAD DE LA REPÚBLICA - URUGUAY

Facultad de Ingeniería / Unidad de Recursos Informáticos

## VÍNCULOS CON LA INSTITUCIÓN

### **Funcionario/Empleado (12/2017 - 09/2021)** Trabajo relevante

40 horas semanales

Se desarrollan tareas profesionales de administración de la red y servicios informáticos de facultad, que incluyen la instalación, mantenimiento y administración de los servicios informáticos centrales de la Facultad de Ingeniería, del Centro Nacional de Supercomputación, ClusterUY, del Cluster FING, de la red inalámbrica de Facultad y de la nueva red de telefonía IP de la Facultad, y la Atención a pedidos de apoyo técnico de los administradores de sistemas locales, usuarios informáticos docentes y estudiantes de la Facultad.

Escalafón: Docente

Grado: Grado 4

Cargo: Interino

### **Funcionario/Empleado (12/2012 - 12/2017)**

40 horas semanales

Escalafón: Docente

Grado: Grado 3

Cargo: Interino

### **Funcionario/Empleado (12/2011 - 12/2012)**

40 horas semanales

Escalafón: Docente

Grado: Grado 2

Cargo: Interino

### **Funcionario/Empleado (11/2007 - 12/2011)**

40 horas semanales

Escalafón: Docente

Grado: Grado 1

Cargo: Interino

### SECTOR EMPRESAS/PRIVADO - EMPRESA PRIVADA - URUGUAY

Tilsor Tecnología Informática

## VÍNCULOS CON LA INSTITUCIÓN

### **Otro (03/2019 - 05/2019)**

Consultor en seguridad informática 10 horas semanales

Participación en proyecto de consultoría y asesoramiento de seguridad informática a ANCAP.

### **Otro (07/2009 - 12/2009)**

Consultor en seguridad informática 10 horas semanales

Participación, como desarrollador y consultor en seguridad informática, en el proyecto "Sistema de Control de Acceso del Plan Ceibal". Las tareas desarrolladas incluyeron el diseño e implementación un protocolo de autenticación, sin usar contraseñas, para todas las XO-1 del Plan Ceibal (más de 300.000) en una red inalámbrica, además de la infraestructura de soporte.

#### CARGA HORARIA

Carga horaria de docencia: 12 horas  
Carga horaria de investigación: 15 horas  
Carga horaria de formación RRHH: 3 horas  
Carga horaria de extensión: 5 horas  
Carga horaria de gestión: 5 horas

## Producción científica/tecnológica

Mi actividad académica se centra en el área de la seguridad informática. Los temas en los que recientemente he desarrollado investigación incluyen seguridad en aplicaciones web, en particular en el estudio y diseño de firewalls de aplicaciones que incorporen técnicas de aprendizaje automático; el modelado y verificación formal de propiedades de seguridad en plataformas de virtualización y dispositivos móviles; y el estudio del impacto en la seguridad y privacidad de soluciones tecnológicas para hacer frente a la pandemia del COVID-19. Otra área en la que he participado ha sido en el estudio de la seguridad en dispositivos de internet de las cosas, en especial en un proyecto en conjunto con UTE en el área de smart grids y con la Intendencia de Montevideo en smart cities.

Además, he liderado el equipo de desarrollo de Tectonic, un cyber range académico creado por el Grupo de Seguridad Informática del InCo para realizar investigación, dictado de cursos de grado y posgrado, y entrenamientos en ciberseguridad a nivel nacional y regional. También he participado en otras actividades de formación de grado y posgrado, como dictado de cursos y tutoría de proyectos de grado; en asesoramiento especializado; y en la difusión y sensibilización sobre la problemática de la seguridad informática en distintos ámbitos.

## Producción bibliográfica

### ARTÍCULOS PUBLICADOS

#### ARBITRADOS

##### **COVID-19 Mobile Applications: A Study of Trackers and Data Leaks (Completo, 2024)**

Nicolas Serrano , G. BETARTE , JUAN DIEGO CAMPO  
Journal of Internet Services and Applications, v.: 15 1 , p.:139 - 159, 2024  
Escrito por invitación  
ISSN: 18674828  
E-ISSN: 18690238  
DOI: <https://doi.org/10.5753/jisa.2024.3882>

WEB OF SCIENCE™ Scopus 

##### **Contact tracing solutions for COVID-19: applications, data privacy and security (Completo, 2022)**

GUSTAVO BETARTE , JUAN DIEGO CAMPO , ANDREA DELGADO , LAURA GONZÁLEZ ,  
ÁLVARO MARTÍN , RODRIGO MARTÍNEZ , BÁRBARA MURACCIOLE  
CLEI Electronic Journal, v.: 25 2022  
Escrito por invitación  
E-ISSN: 07175000  
DOI: [10.19153/cleiej.25.2.4](https://doi.org/10.19153/cleiej.25.2.4)  
<http://dx.doi.org/10.19153/cleiej.25.2.4>

Scopus® latindex 

##### **System-Level Non-interference of Constant-Time Cryptography. Part II: Verified Static Analysis and Stealth Memory (Completo, 2020) Trabajo relevante**

G. BARTHE , G. BETARTE , JUAN DIEGO CAMPO , LUNA, C. , D. PICHARDIE  
Journal of Automated Reasoning, v.: 64 p.:1685 - 1729, 2020  
Medio de divulgación: Internet

ISSN: 01687433  
E-ISSN: 15730670  
DOI: <https://doi.org/10.1007/s10817-020-09548-x>  
WEB OF SCIENCE™ Scopus®

**System-Level Non-interference of Constant-Time Cryptography. Part I: Model (Completo, 2019)** Trabajo relevante

JUAN DIEGO CAMPO , G. BETARTE , G. BARTHE , LUNA, C.  
Journal of Automated Reasoning, v.: 63 1 , p.:1 - 51, 2019  
Areas de conocimiento:  
Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información / Ingeniería de Sistemas y Comunicaciones / Seguridad Informática  
ISSN: 01687433  
E-ISSN: 15730670  
<https://doi.org/10.1007/s10817-017-9441-5>  
WEB OF SCIENCE™ Scopus®

**A formal approach for the verification of the permission-based security model of Android (Completo, 2018)**

JUAN DIEGO CAMPO , LUNA, C. , G. BETARTE , C. Sanz , M. Cristiá , F. Gorostiaga  
CLEI Electronic Journal, v.: 21 2 , 2018  
Escrito por invitación  
E-ISSN: 07175000  
DOI: <https://doi.org/10.19153/cleiej.21.2.3>



**Formal Analysis of Android's Permission-Based Security Model (Completo, 2016)**

JUAN DIEGO CAMPO , Gustavo Betarte , Carlos Luna , Agustín Romano  
Scientific Annals of Computer Science, v.: 26 1 , p.:27 - 68, 2016  
ISSN: 18438121  
E-ISSN: 22482695  
DOI: [10.7561/SACS.2016.1.27](https://doi.org/10.7561/SACS.2016.1.27)  
WEB OF SCIENCE™ Scopus®

**DOCUMENTOS DE TRABAJO**

**Desafíos de seguridad y privacidad en el diseño e implementación de soluciones de rastreo de proximidad: Análisis preliminar de riesgos (2020)**

Completo  
G. BETARTE , JUAN DIEGO CAMPO , A. DELGADO , P. EZZATTI , A. FORTEZZA , L. GONZALEZ , A. MARTIN , B. MURACCIOLE , R. RUGGIA

Palabras clave: COVID19 rastreo digital de proximidad soluciones tecnológicas protección de datos personales seguridad informática análisis de riesgo  
Medio de divulgación: Internet  
<https://www.fing.edu.uy/inco/proyectos/protect/post/chapter-2/>

**Desafíos de seguridad y privacidad en el diseño e implementación de soluciones de rastreo de proximidad (2020)**

Completo  
G. BETARTE , JUAN DIEGO CAMPO , A. DELGADO , P. EZZATTI , A. Fortezza , L. GONZALEZ , A. MARTIN , B. MURACCIOLE , R. RUGGIA

Palabras clave: COVID-19 rastreo digital de proximidad soluciones tecnológicas protección de datos personales seguridad informática  
Medio de divulgación: Internet  
<https://www.fing.edu.uy/inco/proyectos/protect/post/chapter-1/>

**Modelos de memoria en entornos de virtualización (2012)**

Completo  
GUSTAVO BETARTE , JUAN DIEGO CAMPO , MAURICIO CHIMENTO , CARLOS LUNA  
Serie: 12, v: 2

Instituto de Computación  
Palabras clave: Virtualización

Áreas de conocimiento:

Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información / Ingeniería de Sistemas y Comunicaciones / Seguridad Informática

Medio de divulgación: Internet

<http://www.fing.edu.uy/inco/pedeciba/bibliote/reptec/TR1202.pdf>

### **Seguridad informática en la Universidad de la República (2010)**

Completo

GUSTAVO BETARTE , ALEJANDRO BLANCO , JUAN DIEGO CAMPO , MARÍA EUGENIA CORTI , CARLOS LUNA , MARCELO RODRÍGUEZ , FELIPE ZIPITRÍA

Serie: 10, v: 9

Instituto de Computación

Palabras clave: Seguridad Informática

Áreas de conocimiento:

Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información / Ingeniería de Sistemas y Comunicaciones / Seguridad Informática

Medio de divulgación: Internet

<http://www.fing.edu.uy/inco/pedeciba/bibliote/reptec/TR1009.pdf>

### **Generación de ambientes para entrenamiento en seguridad informática (2009)** Trabajo relevante

Completo

JUAN DIEGO CAMPO , ALEJANDRO BLANCO , LUCÍA ESCANELLAS , CARLOS PINTADO , MARCELO RODRÍGUEZ

Serie: 09, v: 7

Instituto de Computación

Palabras clave: Seguridad Informática Laboratorios de Seguridad Virtualización

Áreas de conocimiento:

Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información / Ingeniería de Sistemas y Comunicaciones / Seguridad Informática

Medio de divulgación: Internet

<http://www.fing.edu.uy/inco/pedeciba/bibliote/reptec/TR0907.pdf>

## **PUBLICACIÓN DE TRABAJOS PRESENTADOS EN EVENTOS**

### **Process Mining-Based Assessment of Cyber Range Trainings (2024)**

G. Guerrero , G. BETARTE , JUAN DIEGO CAMPO

Publicado

Completo

Evento: Regional

Descripción: Latin American Computer Conference (CLEI)

Ciudad: Bahía Blanca, Argentina

Año del evento: 2024

Publicación arbitrada

DOI: <https://doi.org/10.1109/CLEI64178.2024.10700452>

### **Tectonic: An Academic Cyber Range (2024)**

G. Guerrero , G. BETARTE , JUAN DIEGO CAMPO

Publicado

Completo

Evento: Nacional

Descripción: IEEE Biennial Congress of Argentina (ARGENCON)

Ciudad: San Nicolás de los Arroyos, Argentina

Año del evento: 2024

Anales/Proceedings: 2024 IEEE Biennial Congress of Argentina (ARGENCON)

Publicación arbitrada

DOI: [10.1109/ARGENCON62399.2024.10735713](https://doi.org/10.1109/ARGENCON62399.2024.10735713)

### **Third-Party Trackers in COVID-19 Mobile Applications Can Enable Privacy Leaks (2023)**

JUAN DIEGO CAMPO , G. BETARTE , N. SERRANO

Publicado

Completo

Evento: Regional  
Descripción: Latin-American Symposium on Dependable and Secure Computing  
Ciudad: La Paz, Bolivia  
Año del evento: 2023  
Anales/Proceedings:LADC '23: Proceedings of the 12th Latin-American Symposium on Dependable and Secure Computing  
Pagina inicial: 80  
Pagina final: 89  
Publicación arbitrada  
Areas de conocimiento:  
Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información / Ingeniería de Sistemas y Comunicaciones / Seguridad Informática  
Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información / Ingeniería de Sistemas y Comunicaciones / Privacidad  
Medio de divulgación: Internet  
DOI: <https://doi.org/10.1145/3615366.3615426>

#### **Proximity tracing applications for COVID-19: data privacy and security (2021)**

JUAN DIEGO CAMPO , G. BETARTE , Andrea Delgado , Pablo Ezzatti , Laura Gonzalez , ÁLVARO MARTÍN , R. MARTÍNEZ , Bárbara Muracciole  
Publicado  
Completo  
Evento: Regional  
Descripción: Simposio Latinoamericano de Informática y Sociedad - CLEI  
Año del evento: 2021  
Publicación arbitrada  
<https://clei2021.cr/>

#### **A certified reference validation mechanism for the permission model of Android (2017)**

JUAN DIEGO CAMPO , Gustavo Betarte , Carlos Luna , Felipe Gorostiaga  
Publicado  
Completo  
Evento: Internacional  
Descripción: Logic-based Program Synthesis and Transformation (LOPSTR)  
Ciudad: Namur  
Año del evento: 2017  
Publicación arbitrada

#### **Towards formal model-based analysis and testing of Android's security mechanisms (2017)**

JUAN DIEGO CAMPO , G. BETARTE , Carlos Luna , Maximiliano Cristiá , Felipe Gorostiaga , Camila Sanz  
Publicado  
Completo  
Evento: Regional  
Descripción: Conferencia Latinoamericana de Informática  
Año del evento: 2017  
Publicación arbitrada

#### **Verifying Android's Permission Model (2015)**

G. BETARTE , JUAN DIEGO CAMPO , LUNA, C. , Agustin ROMANO  
Publicado  
Completo  
Descripción: International Colloquium on Theoretical Aspects of Computing (ICTAC)  
Año del evento: 2015  
Anales/Proceedings:Lecture Notes in Computer Science  
Volumen:9399  
Pagina inicial: 485  
Pagina final: 504  
DOI: [10.1007/978-3-319-25150-9\\_28](https://doi.org/10.1007/978-3-319-25150-9_28)  
Scopus

#### **System-level non-interference for constant-time cryptography (2014)** Trabajo relevante

GILLES BARTHE , GUSTAVO BETARTE , JUAN DIEGO CAMPO , CARLOS LUNA , DAVID PICHARDIE

Publicado  
Completo  
Evento: Internacional  
Descripción: 21st ACM Conference on Computer and Communications Security  
Ciudad: Scottsdale, Arizona, USA  
Año del evento: 2014  
Publicación arbitrada  
Palabras clave: Information flow control non-interference cache-based attacks constant-time cryptography stealth memory Coq  
Areas de conocimiento:  
Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información / Ingeniería de Sistemas y Comunicaciones / Seguridad Informática  
DOI: [10.1145/2660267.2660283](https://doi.org/10.1145/2660267.2660283)

Cache-based attacks are a class of side-channel attacks that are particularly effective in virtualized or cloud-based environments, where they have been used to recover secret keys from cryptographic implementations. One common approach to thwart cache-based attacks is to use constant-time implementations, i.e. which do not branch on secrets and do not perform memory accesses that depend on secrets. However, there is no rigorous proof that constant-time implementations are protected against concurrent cache-attacks in virtualization platforms with shared cache; moreover, many prominent implementations are not constant-time. An alternative approach is to rely on system-level mechanisms. One recent such mechanism is stealth memory, which provisions a small amount of private cache for programs to carry potentially leaking computations securely. Stealth memory induces a weak form of constant-time, called S-constant-time, which encompasses some widely used cryptographic implementations. However, there is no rigorous analysis of stealth memory and S-constant-time, and no tool support for checking if applications are S-constant-time. We propose a new information-flow analysis that checks if an x86 application executes in constant-time, or in S-constant-time. Moreover, we prove that constant-time (resp. S-constant-time) programs do not leak confidential information through the cache to other operating systems executing concurrently on virtualization platforms (resp. platforms supporting stealth memory). The soundness proofs are based on new theorems of independent interest, including isolation theorems for virtualization platforms (resp. platforms supporting stealth memory), and proofs that constant-time implementations (resp. S-constant-time implementations) are non-interfering with respect to a strict information flow policy which disallows that control flow and memory accesses depend on secrets. We formalize our results using the Coq proof assistant and we demonstrate the effectiveness of our analyses on cryptographic implementations, including PolarSSL AES, DES and RC4, SHA256 and Salsa20.

Scopus

### Formally Verified Implementation of an Idealized Model of Virtualization (2013)

G. BARTHE , G. BETARTE , JUAN DIEGO CAMPO , M. CHIMENTO , LUNA, C.  
Publicado  
Completo  
Descripción: 19th International Conference on Types for Proofs and Programs (TYPES)  
Ciudad: Toulouse, France  
Año del evento: 2013  
Volumen:26  
Pagina inicial: 45  
Pagina final: 63  
Publicación arbitrada  
DOI: [10.4230/LIPICS.TYPES.2013.45](https://doi.org/10.4230/LIPICS.TYPES.2013.45)

### Cache-leakage Resilience Isolation in an Idealized Model of Virtualization (2012) Trabajo relevante

GILLES BARTHE , GUSTAVO BETARTE , JUAN DIEGO CAMPO , CARLOS LUNA  
Publicado  
Completo  
Evento: Internacional  
Descripción: 25th IEEE Computer Security Foundations Symposium  
Ciudad: Cambridge MA, USA  
Año del evento: 2012  
Publicación arbitrada  
Palabras clave: Virtualización Side Channels Cache  
Areas de conocimiento:  
Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información / Ingeniería de Sistemas y Comunicaciones /  
Medio de divulgación: Internet

### **Formally Verifying Isolation and Availability in an Idealized Model of Virtualization (2011)**

G. BARTHE , G. BETARTE , JUAN DIEGO CAMPO , LUNA, C.

Publicado

Completo

Descripción: FM 2011: Formal Methods - 17th International Symposium on Formal Methods

Ciudad: Limerick, Ireland

Año del evento: 2011

Anales/Proceedings: Lecture Notes in Computer Science

Volumen:6664

Página inicial: 231

Página final: 245

Publicación arbitrada

Editorial: Springer

DOI: [10.1007/978-3-642-21437-0\\_19](https://doi.org/10.1007/978-3-642-21437-0_19)

[Scopus](#)

### **Generación de Ambientes para Entrenamiento en Seguridad Informática (2009)**

JUAN DIEGO CAMPO , ALEJANDRO BLANCO , LUCÍA ESCANELLAS , CARLOS PINTADO , MARCELO RODRÍGUEZ

Publicado

Completo

Evento: Internacional

Descripción: V Congreso Iberoamericano de Seguridad Informática

Ciudad: Montevideo

Año del evento: 2009

Publicación arbitrada

Palabras clave: Seguridad Informática Laboratorios de Seguridad Virtualización

Áreas de conocimiento:

Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información / Ingeniería de Sistemas y Comunicaciones / Seguridad Informática

Medio de divulgación: CD-Rom

[http://www.fing.edu.uy/inco/eventos/cibsi09/docs/Papers/CIBSI-Dia3-Sesion8\(3\).pdf](http://www.fing.edu.uy/inco/eventos/cibsi09/docs/Papers/CIBSI-Dia3-Sesion8(3).pdf)

## **Producción técnica**

### **PRODUCTOS**

#### **Tectonic: un Cyber Range académico (2024)**

Producto, Software

JUAN DIEGO CAMPO

Tectonic es un cyber range diseñado por el GSI para proporcionar escenarios realistas de ciberseguridad para la educación y la formación, a través del despliegue de redes, sistemas y aplicaciones que pueden utilizarse para capacitar a los usuarios en temas de ciberseguridad. Sus funcionalidades clave incluyen configuraciones de red personalizables, monitoreo en tiempo real y simulaciones automatizadas de ataques. Incorpora herramientas existentes del enfoque de infraestructura como código (IaC), lo que permite especificar todos los componentes de un escenario de ciberseguridad de manera declarativa. Esta especificación se realiza en un lenguaje de alto nivel que puede ser interpretado y permite la generación automática de escenarios sobre la plataforma subyacente del laboratorio. Las descripciones declarativas de los escenarios facilitan su versionado, mantenimiento y compartición, promoviendo la colaboración con otras instituciones y laboratorios de este tipo. Tectonic es software libre y abierto, y se ha utilizado en diferentes cursos de ciberseguridad de grado y de posgrado, así como en diversas actividades de formación en Uruguay y América Latina.

País: Uruguay

Producto con aplicación productiva o social: Tectonic ha sido utilizado como

<https://github.com/GSI-Fing-Udelar/tectonic>

### **OTRAS PRODUCCIONES**

### **ORGANIZACIÓN DE EVENTOS**

#### **9th IEEE International Conference on Software Engineering and Formal Methods (2011)**

JUAN DIEGO CAMPO

Congreso

Sub Tipo: Organización

Lugar: Uruguay ,Montevideo

Idioma: Inglés

Duración: 1 semanas

Evento itinerante: SI

Institución Promotora/Financiadora: IEEE

Areas de conocimiento:

Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información /

Ingeniería de Sistemas y Comunicaciones / Métodos Formales

Información adicional: Participación como ayudante en la organización local de la conferencia.

## Evaluaciones

### EVALUACIÓN DE PUBLICACIONES

#### REVISIONES

##### **Journal of Supercomputing ( 2021 / 2022 )**

Tipo de publicación: Revista

Cantidad: Menos de 5

### EVALUACIÓN DE EVENTOS Y CONGRESOS

##### **LV Simpósio Brasileiro de Pesquisa Operacional ( 2023 )**

Revisiones

Brasil

##### **International Symposium on Formal Methods ( 2023 )**

Revisiones

##### **Latin-American Symposium on Dependable and Secure Computing - Fast Abstracts Track ( 2023 / 2024 )**

Comité programa congreso

Arbitrado

##### **Latin American Conference on Computational Intelligence ( 2022 )**

Comité programa congreso

Arbitrado

##### **Simposio Latinoamericano de Teoría de la Computación ( 2021 / 2022 )**

Comité programa congreso

Arbitrado

##### **Simpósio Latinoamericano de Infraestrutura, Hardware y Software ( 2021 / 2022 )**

Comité programa congreso

Arbitrado

Simposio asociado a la Conferencia Latinoamericana de Informática (CLEI)

**International Symposium on Formal Methods ( 2021 )**

Revisiones

**Simposio Latinoamericano de Infraestructura, Hardware y Software ( 2020 )**

Revisiones

Ecuador

**International Symposium on Formal Methods ( 2019 )**

Revisiones

Portugal

**Simposio Latinoamericano de Infraestructura, Hardware y Software ( 2018 )**

Revisiones

Brasil

Arbitrado

**IEEE URUCON 2017 ( 2017 )**

Revisiones

Uruguay

IEEE

**International Colloquium on Theoretical Aspects of Computing ( 2015 )**

Revisiones

Colombia

**Asia Pacific Network Operations and Management Symposiu ( 2015 )**

Revisiones

Corea del Sur

**INSTITUCIONES Y CARRERAS**

**Tipo de evaluación Carrera / Especialización/Perfeccionamiento ( 01/01/2021 / 01/01/2021 )**

Par nacional

Universidad ORT Uruguay - Facultad de Ingeniería , Uruguay

Diploma de Especialización en Ciberseguridad

**EVALUACIÓN DE PREMIOS**

**Concurso de Proyectos Finales y Tesis de Postgrado de Ingeniería ( 2017 )**

Evaluación de premios y concursos

Uruguay

Cantidad: Menos de 5

Academia Nacional de Ingeniería del Uruguay

**JURADO DE TESIS**

**Maestría en Ingeniería en Computación ( 2021 )**

Jurado de mesa de evaluación de tesis

Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería / Instituto de Computación , Uruguay  
Nivel de formación: Maestría

## Formación de RRHH

### TUTORÍAS CONCLUIDAS

#### POSGRADO

##### **Detection and Classification of Privacy Leaks Enabled by Third-Party Trackers in COVID-19 Mobile Applications (2021 - 2023)**

Tesis de maestría  
Sector Educación Superior/Público / Programa de Desarrollo de las Ciencias Básicas / Área Informática (PEDECIBA) , Uruguay  
Programa: Maestría en Informática  
Tipo de orientación: Cotutor ( JUAN DIEGO CAMPO , G. BETARTE )  
Nombre del orientado: Nicolás Serrano  
País: Uruguay

#### GRADO

##### **WAF NextGen (2020 - 2021)**

Tesis/Monografía de grado  
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería / Instituto de Computación , Uruguay  
Programa: Ingeniería en Computación  
Tipo de orientación: Cotutor en pie de igualdad ( JUAN DIEGO CAMPO )  
Nombre del orientado: Juan Pablo Martínez, Ignacio Monzalvo  
País: Uruguay  
Áreas de conocimiento:  
Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información / Ingeniería de Sistemas y Comunicaciones / Seguridad Informática

##### **Contramedidas para la manipulación maliciosa de dispositivos ciberfísicos (2019 - 2020)**

Tesis/Monografía de grado  
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería / Instituto de Computación , Uruguay  
Programa: Ingeniería en Computación  
Tipo de orientación: Cotutor en pie de igualdad ( JUAN DIEGO CAMPO , G. BETARTE )  
Nombre del orientado: Martín Pacheco y Sebastián Passaro  
País: Uruguay  
Áreas de conocimiento:  
Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información / Ingeniería de Sistemas y Comunicaciones / Seguridad Informática

##### **Análisis de seguridad y especificación de controles para una red de dispositivos inteligentes**

Tesis/Monografía de grado  
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería / Instituto de Computación , Uruguay  
Tipo de orientación: Cotutor en pie de igualdad  
Nombre del orientado: Joaquín Marquez y Gabriel Rodríguez  
País: Uruguay  
Áreas de conocimiento:  
Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información / Ingeniería de Sistemas y Comunicaciones / Seguridad Informática

##### **Razonando sobre la seguridad de Android**

Tesis/Monografía de grado  
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería , Uruguay  
Programa: Ingeniería en Computación  
Tipo de orientación: Cotutor en pie de igualdad  
Nombre del orientado: Camila Sanz

País: Uruguay

Areas de conocimiento:

Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información / Ingeniería de Sistemas y Comunicaciones / Seguridad Informática

#### **Especificación y verificación formal de algoritmos críticos en un modelo de virtualización**

Tesis/Monografía de grado

Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería , Uruguay

Programa: Ingeniería en Computación

Nombre del orientado: Mauricio Martínez y Enrique Rodríguez

País: Uruguay

Areas de conocimiento:

Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información / Ingeniería de Sistemas y Comunicaciones / Seguridad Informática

#### **Verificación formal de propiedades de seguridad en modelos de virtualización**

Tesis/Monografía de grado

Sector Extranjero/Internacional/Otros / Facultad de Ciencias Exactas, Ingeniería y Agrimensura - UNR , Argentina

Programa: Licenciatura en Ciencias de la Computación

Nombre del orientado: Mauricio Chimento

País: Argentina

Palabras Clave: Virtualización No interferencia

Areas de conocimiento:

Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información / Ingeniería de Sistemas y Comunicaciones / Métodos Formales

Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información / Ingeniería de Sistemas y Comunicaciones / Seguridad Informática

#### **Especificación y Verificación formal de un modelo de virtualización: Prueba de safety de validez de estados y construcción de un prototipo certificado de hypervisor**

Tesis/Monografía de grado

Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería , Uruguay

Programa: Ingeniería en Computación

Nombre del orientado: Julio Pérez Ares

País: Uruguay

Palabras Clave: Virtualización

Areas de conocimiento:

Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información / Ingeniería de Sistemas y Comunicaciones / Seguridad Informática

Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información / Ingeniería de Sistemas y Comunicaciones / Métodos Formales

### **TUTORÍAS EN MARCHA**

#### **POSGRADO**

##### **Monitoreo y evaluación del comportamiento de usuarios en un cyber range (2022)**

Tesis de maestría

Sector Educación Superior/Público / Programa de Desarrollo de las Ciencias Básicas / Área Informática (PEDECIBA) , Uruguay

Programa: Maestría en Informática

Tipo de orientación: Cotutor

Nombre del orientado: Guillermo Guerrero

País/Idioma: Uruguay,

#### **GRADO**

##### **Generación de laboratorios de Sistemas de Control Industrial sobre Cyber Ranges (2025)**

Tesis/Monografía de grado

Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería / Instituto de Computación , Uruguay

Programa: Ingeniería en Computación

Tipo de orientación: Cotutor  
Nombre del orientado: Nicolas Adrién y Agustin Britos  
País/Idioma: Uruguay,

#### **Generación de laboratorios de análisis forense digital y gestión de incidentes sobre Cyber Ranges (2025)**

Tesis/Monografía de grado  
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería / Instituto de Computación , Uruguay  
Programa: Ingeniería en Computación  
Tipo de orientación: Cotutor  
Nombre del orientado: Rodrigo Aguillón e Ignacio Alesina  
País/Idioma: Uruguay,

#### **WACE: Un Integrador de Clasificadores de Ataques Web (2024)**

Tesis/Monografía de grado  
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería / Instituto de Computación , Uruguay  
Programa: Ingeniería en Computación  
Tipo de orientación: Cotutor  
Nombre del orientado: Agustín de León y Tobias Iroa  
País/Idioma: Uruguay,

#### **Emulación de Dispositivos Android en un Cyber Range (2024)**

Tesis/Monografía de grado  
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería / Instituto de Computación , Uruguay  
Programa: Ingeniería en Computación  
Tipo de orientación: Cotutor  
Nombre del orientado: Nicolás Vidal y Federico Correa  
País/Idioma: Uruguay,

## Otros datos relevantes

### PREMIOS, HONORES Y TÍTULOS

#### **Premio a la mejor de tesis de Doctorado del PEDECIBA Informática (2017)**

(Nacional)  
PEDECIBA

### PRESENTACIONES EN EVENTOS

#### **Congreso Nacional de Ciencias de la Computación de Bolivia (CCBOL) (2024)**

Congreso  
Ponencia: Tectonic: un Cyber Range académico  
Bolivia  
Tipo de participación: Conferencista invitado  
Nombre de la institución promotora: Universidad Mayor Real y Pontificia de San Francisco Xavier de Chuquisaca  
Alcance geográfico: Nacional

#### **Coloquio de Ciberseguridad CIC (2024)**

Seminario  
Conferencia magistral "Educación integral en ciberseguridad: El papel fundamental de la capacitación práctica y las plataformas de entrenamiento"  
México  
Tipo de participación: Conferencista invitado  
Nombre de la institución promotora: Instituto Politécnico Nacional de México  
Alcance geográfico: Nacional

#### **Workshop Ciberseguridad: metodología, técnicas y herramientas (2024)**

Seminario  
Título de la charla: "Tectonic: un Cyber Range académico"  
Uruguay  
Tipo de participación: Expositor oral  
Nombre de la institución promotora: Grupo de Seguridad Informática, Instituto de Computación, Universidad de la República  
Alcance geográfico: Nacional

**Hacia una visión integrada y transversal del estado de la Ciberseguridad en América Latina y el Caribe (2023)**

Otra  
Ponencia "Plataformas de entrenamiento en ciberseguridad"  
Tipo de participación: Conferencista invitado  
Nombre de la institución promotora: CLEI - CiberLAC  
Alcance geográfico: Regional

**Seminario sobre seguridad IoT y ciudades inteligentes (2019)**

Seminario  
Presentación sobre la problemática de botnets de dispositivos IoT de alto consumo en la red eléctrica  
Uruguay  
Tipo de participación: Expositor oral  
Nombre de la institución promotora: Intendencia de Montevideo y Facultad de Ingeniería, Universidad de la República Se presentaron los resultados del artículo BlackIoT: IoT Botnet of High Wattage Devices Can Disrupt the Power Grid, por Saleh Soltan, Prateek Mittal, and H. Vincent Poor, 27th USENIX Security Symposium, 2018

**Seminario sobre seguridad IoT y smart grids (2018)**

Seminario  
Presentación sobre la problemática de botnets de dispositivos IoT de alto consumo en la red eléctrica  
Uruguay  
Tipo de participación: Expositor oral  
Nombre de la institución promotora: UTE y Facultad de Ingeniería, Universidad de la República Se presentaron los resultados del artículo BlackIoT: IoT Botnet of High Wattage Devices Can Disrupt the Power Grid, por Saleh Soltan, Prateek Mittal, and H. Vincent Poor, 27th USENIX Security Symposium, 2018

**Latin American Workshop on Formal Methods (2013)**

Taller  
VirtualCert: A Certified Idealized Model of Virtualization  
Argentina  
Tipo de participación: Expositor oral

**Ciclo de charlas CERTificate! 2010 (2010)**

Encuentro  
Framework para el entrenamiento en seguridad informática  
Uruguay  
Tipo de participación: Expositor oral  
Nombre de la institución promotora: CERTuy

**XI Jornadas de Informática e Investigación Operativa (2010)**

Encuentro  
Diseño e Implementación de Ambientes para el Entrenamiento en Seguridad Informática  
Uruguay  
Tipo de participación: Expositor oral  
Nombre de la institución promotora: Instituto de Computación, Facultad de Ingeniería, Universidad de la República

**X Jornadas de Informática e Investigación Operativa (2008)**

Encuentro  
Design and Development of a Framework for IT-Security Training  
Uruguay

Tipo de participación: Expositor oral

Nombre de la institución promotora: Instituto de Computación, Facultad de Ingeniería, Universidad de la República

## Indicadores de producción

<b>ACTIVIDADES</b>	<b>36</b>
Líneas de investigación	6
Proyectos Investigación Desarrollo	7
Docencia	6
Extensión	2
Gestión Académica	4
Capacitación Entrenamiento	4
Servicio Técnico Especializado	1
Pasantía	1
Otra Actividad Técnica	5
<b>PRODUCCIÓN BIBLIOGRÁFICA</b>	<b>23</b>
Artículos publicados en revistas científicas	6
Completo	6
Trabajos en eventos	12
Documentos de trabajo	5
Completo	5
<b>PRODUCCIÓN TÉCNICA</b>	<b>2</b>
Productos tecnológicos	1
Otros tipos	1
<b>EVALUACIONES</b>	<b>15</b>
Evaluación de eventos	13
Evaluación de publicaciones	1
Jurado de tesis	1
<b>FORMACIÓN RRHH</b>	<b>13</b>
Tutorías/Orientaciones/Supervisiones concluidas	8
Tesis/Monografía de grado	7
Tesis de maestría	1
Tutorías/Orientaciones/Supervisiones en marcha	5
Tesis de maestría	1
Tesis/Monografía de grado	4

