



GUSTAVO BETARTE GUIDI

Dr. Ing.

[gustun@fing.edu.uy](mailto:gustun@fing.edu.uy)  
<http://www.fing.edu.uy/~gustun>

Julio Herrera y Reissig 565,  
 Piso 5, CP 11300, Montevideo,  
 Uruguay  
 21742714 - Extensión

**SNI**

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

Categorización actual: Nivel II (Activo)

Fecha de publicación: 21/04/2026  
 Última actualización: 21/04/2026

**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: J.Herrera y Reissig 565 / 11300

País: Uruguay / Montevideo / Montevideo

Teléfono: (5982) 7142714 / 10126

Correo electrónico/Sitio Web: [gustun@fing.edu.uy](mailto:gustun@fing.edu.uy) <http://www.fing.edu.uy/~gustun>

**Formación****Formación académica****CONCLUIDA****DOCTORADO****Doktor i Datavetenskap (1993 - 1997)**

Gothenburg University , Suecia

Título de la disertación/tesis/defensa: Dependent Record Types and Algebraic Structures in Type Theory

Tutor/es: Dr. Björn von Sydow

Obtención del título: 1998

Sitio web de la disertación/tesis/defensa: <http://hdl.handle.net/2077/14871>

Financiación:

Gothenburg University , Suecia

Palabras Clave: Type Theory, Dependent Records, Subtyping

Áreas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Teoría de Tipos, Logical Frameworks

**MAESTRÍA****Licenciat i Datavetenskap (1992 - 1993)**

Gothenburg University , Suecia

Título de la disertación/tesis/defensa: A case study in machine-assisted proofs: The Integers form an Integral Domain

Tutor/es: Dr. Björn von Sydow

Obtención del título: 1994

Sitio web de la disertación/tesis/defensa:

<http://www.fing.edu.uy/%7Egustun/Publications/thesis/lic.ps.gz>

Financiación:

Gothenburg University , Suecia

Palabras Clave: Type Theory, Constructive Integers

Áreas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Teoría de Tipos, Logical Frameworks

**Maestría en Informática (UDELAR-PEDECIBA) (1992 - 1993)**

Universidad de la República - Facultad de Ingeniería , Uruguay

Título de la disertación/tesis/defensa: A case study in machine-assisted proofs: The Integers form an Integral Domain

Tutor/es: Dr. Bjorn von Sydow - MSc Juan José Cabezas

Obtención del título: 1994

Sitio web de la disertación/tesis/defensa:

<http://www.fing.edu.uy/%7Egustun/Publications/thesis/lic.ps.gz>

Palabras Clave: Logical Frameworks, Formalización

Areas de conocimiento:

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

## **GRADO**

### **Ingeniero de Sistemas en Computación (1983 - 1990)**

Universidad de la República - Facultad de Ingeniería , Uruguay

Título de la disertación/tesis/defensa:

Obtención del título: 1990

Areas de conocimiento:

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

### **Analista Programador (1983 - 1986)**

Universidad de la República - Facultad de Ingeniería , Uruguay

Título de la disertación/tesis/defensa:

Obtención del título: 1987

Areas de conocimiento:

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

## Formación complementaria

### **CONCLUIDA**

## **POSDOCTORADOS**

### **FORMAVIE: Modélisation Formelle et Certification Sécuritaire pour Machine Virtuelle Embarquée (2001 - 2002)**

Sector Extranjero/Internacional/Otros / Ministère des Finances - France , Francia

Palabras Clave: Máquina Virtual, Java Card, Seguridad

Areas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Sistemas Embebidos, Semántica Formal

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

## **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

### **Francés**

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

### **Sueco**

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

### **Portugués**

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

## Áreas de actuación

### CIENCIAS NATURALES Y EXACTAS

Ciencias de la Computación e Información /Ciencias de la Computación /Lógica de la Programación, Métodos Formales, Seguridad Informática

### INGENIERÍA Y TECNOLOGÍA

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

## Actuación profesional

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

Área Informática (PEDECIBA) / Instituto de Computación, Facultad de Ingeniería, Udelar

### VÍNCULOS CON LA INSTITUCIÓN

#### Colaborador (12/2024 - a la fecha) Trabajo relevante

Grado 5 10 horas semanales

#### Colaborador (01/1998 - 12/2024)

Investigador Grado 4 20 horas semanales

#### Colaborador (04/2010 - 02/2020)

Consejo científico del Área de Informática 4 horas semanales

### ACTIVIDADES

#### LÍNEAS DE INVESTIGACIÓN

##### Lógica de la Programación, Teoría Constructiva de Tipos, Verificación Formal (01/1998 - a la fecha )

6 horas semanales

Facultad de Ingeniería, Instituto de Computación , Integrante del equipo

Equipo: WWW.FING.EDU.UY/INCO/MF

Palabras clave: Métodos Formales, Seguridad Sistemas Embebidos

Áreas de conocimiento:

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

##### Seguridad Informática (03/2006 - a la fecha )

10 horas semanales

Facultad de Ingeniería, Instituto de Computación , Coordinador o Responsable

Equipo: WWW.FING.EDU.UY/INCO/GSI

Palabras clave: Seguridad Informática

Áreas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Seguridad Informática

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

### DOCENCIA

#### (09/2005 - a la fecha)

Maestría

Asignaturas:

Taller de Producción de Programas sin Fallas, 10 horas, Teórico-Práctico

Areas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Teoría de Tipos, Logical Frameworks

**(04/2007 - a la fecha)**

Maestría

Asignaturas:

Fundamentos de la Seguridad Informática, 12 horas, Teórico-Práctico

Areas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Seguridad Informática

**(09/1998 - 12/1999 )**

Maestría

Asignaturas:

Compilación de Lenguajes Funcionales Perezosos, 10 horas, Teórico-Práctico

Areas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Compilación de Lenguajes Funcionales

**GESTIÓN ACADÉMICA**

**Miembro del Consejo Científico del Área Informática del Pedeciba (03/2012 - 02/2020 )**

Facultad de Ingeniería - UDELAR, Instituto de Computación

Gestión de la Investigación 3 horas semanales

**Coordinador del Área Informática (02/2018 - 02/2020 )**

Facultad de Ingeniería, Instituto de Computación

Gestión de la Investigación 10 horas semanales

Areas de conocimiento:

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

**Miembro de la Comisión Directiva (02/2018 - 02/2020 )**

Gestión de la Investigación 3 horas semanales

**Coordinador del Área Informática del Pedeciba (04/2010 - 03/2012 )**

Facultad de Ingeniería - UDELAR, Instituto de Computación

Gestión de la Investigación

**Miembro de la Comisión Directiva (04/2010 - 03/2012 )**

Área Informática

Gestión de la Investigación

**Coordinador del Área Informática del Pedeciba (07/2000 - 03/2001 )**

Facultad de Ingeniería, Instituto de Computación

Gestión de la Investigación

Areas de conocimiento:

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

**Coordinador alternativo del Área Informática del Pedeciba (07/1999 - 06/2000 )**

Facultad de Ingeniería, Instituto de Computación

Gestión de la Investigación

Areas de conocimiento:

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

## Tilsor Tecnología Informática

### VÍNCULOS CON LA INSTITUCIÓN

#### Funcionario/Empleado (03/2012 - a la fecha)

Responsable del CSIRT Tilsor 4 horas semanales

#### Funcionario/Empleado (11/2004 - a la fecha) Trabajo relevante

Director de Consultoría 20 horas semanales

### ACTIVIDADES

#### LÍNEAS DE INVESTIGACIÓN

#### Modelos y herramientas para la definición e implantación de mecanismos de control de acceso en sistemas de información (03/2009 - a la fecha )

Mixta

10 horas semanales

Tilsor, Consultoría Tecnológica - Equipo de Seguridad Informática , Coordinador o Responsable  
Equipo: R. MARTÍNEZ

Palabras clave: Control de acceso, modelos, automatización

Áreas de conocimiento:

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

#### Métodos y herramientas para la automatización de análisis de vulnerabilidades de sistemas computacionales (03/2011 - a la fecha )

El drástico incremento de ataques informáticos obliga a los gobiernos, organizaciones y empresas, sin importar su tamaño o actividad, a considerar la seguridad de la información y de la infraestructura informática que brinda soporte a la misma como un tema prioritario. Uno de los mecanismos tradicionales para mantener relativamente seguros los sistemas es realizar auditorías continuas. Debido a la diversidad, multiplicidad y la continua innovación de los sistemas actuales, dichas auditorías caducan cada vez más rápidamente, por lo que hay que se torna necesario automatizar procesos y generar herramientas que asistan a los administradores de sistemas, auditores y analistas de seguridad en esta tarea. Una de las estrategias defensivas claves para garantizar el correcto aseguramiento y configuración de las infraestructuras y aplicaciones informáticas es aplicar la denominada técnica de Hardening de sistemas, que consiste en remover servicios vulnerables e innecesarios, eliminar problemas de seguridad conocidos, configurar adecuadamente todos los dispositivos y asegurar los controles de acceso. Este proceso involucra realizar una evaluación y auditoría de la arquitectura de seguridad de la organización con el fin de desarrollar e implementar procedimientos de consolidación para asegurar sus recursos críticos. Estos procedimientos son personalizados, pero muchas de las tareas pueden automatizarse. Contar con herramientas adecuadas, que provean soporte al proceso de auditoría y faciliten la detección de las problemáticas se torna esencial.

Mixta

10 horas semanales

Área de Consultoría Tecnológica, Equipo de Seguridad Informática , Coordinador o Responsable  
Equipo: M. RODRÍGUEZ , R. MARTÍNEZ

Palabras clave: Análisis de vulnerabilidades, soporte automatizado

Áreas de conocimiento:

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

#### Desarrollo de técnicas de aprendizaje automático y minería de datos para el aseguramiento de sistemas informáticos (07/2015 - a la fecha )

El drástico incremento de ataques informáticos obliga a los gobiernos, organizaciones y empresas, a considerar la seguridad de la información, de las aplicaciones y de la infraestructura informática como un tema prioritario. Una estrategia (defensiva) clave para garantizar el correcto aseguramiento y configuración de las aplicaciones informáticas incluye, entre otros, la utilización de técnicas de desarrollo seguro de código, testeos de seguridad de la aplicación y aseguramiento de la

infraestructura sobre la que se ejecuta. Debido a la diversidad, multiplicidad y la continua innovación de los sistemas actuales se torna necesario automatizar procesos y generar herramientas que asistan a los desarrolladores, administradores de sistemas, auditores y analistas de seguridad en esta tarea. El proyecto WAFINTL tiene como objetivo general la concepción y desarrollo de mecanismos automatizados de identificación, así como el análisis y prevención de ataques informáticos de las aplicaciones web. También se enfocará en el desarrollo de procesos de ciber-inteligencia que provean soporte para el tratamiento sistematizado de las tareas de análisis. El resultado tecnológico del proyecto serán prototipos de herramientas que permitan dar soporte automatizado a esos mecanismos.

Aplicada

6 horas semanales

Tilsor SA, Equipo de Seguridad Informática, Integrante del equipo

Equipo: E. GIMÉNEZ, R. MARTÍNEZ, A. PARDO, N. MONTES, J. GOYENECHÉ

Palabras clave: Seguridad de Aplicaciones Web Aprendizaje automático Minería de datos

Áreas de conocimiento:

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

## **PROYECTOS DE INVESTIGACIÓN Y DESARROLLO**

### **SECUREit (03/2010 - a la fecha)**

Tilsor SECUREit es un framework para la definición e implantación de políticas de control de acceso para sistemas de información. Este framework ha sido, en particular, utilizado para implementar los mecanismos de control de acceso del nuevo Sistema Informático para la Infancia (SIPI). El nuevo sistema SIPI fue desarrollada por Tilsor SA para el INAU respondiendo a una licitación convocada por el programa INFAMILIA del MIDES. Debido a la sensibilidad de la información y requerimientos de seguridad presentados por INAU, se ha desarrollado en el marco del proyecto, un módulo de Control de Acceso basado en RBAC (Role Based Access Control) jerárquico, que además de proveer los mecanismos para modelar y aplicar políticas de control de acceso basada en roles y herencia de privilegios, permite además definir privilegios basados en el contexto de ejecución de la aplicación y en el contenido de los datos sobre las que actúa la misma. Asimismo el framework brinda soporte para implementar visualización controlada de la información. Este sistema ha sido puesto en producción en febrero de 2010. El equipo de Seguridad de Tilsor es el responsable de proveer los servicios de mantenimiento correctivo y evolutivo del sistema. Actualmente se está trabajando en generar una versión de SECUREit que permita proveer los mecanismos de control de acceso como servicios a ser consumidos por un sistema de información independientemente de la tecnología que se haya utilizado para desarrollar al mismo así como de la plataforma en que es ejecutado.

6 horas semanales

Área de Consultoría Tecnológica, Equipo de Seguridad Informática

Desarrollo

Coordinador o Responsable

En Marcha

RRHH formados en el proyecto:

Especialización: 1

Maestría/Magister: 1

Equipo: R. MARTÍNEZ, R. LÓPEZ

Palabras clave: Control de acceso, modelos, automatización

Áreas de conocimiento:

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

### **SATKit - A Security Analysis Toolkit (03/2013 - a la fecha)**

Una de las estrategias defensivas claves para garantizar el correcto aseguramiento y configuración de las infraestructuras y aplicaciones informáticas es aplicar la denominada técnica de Hardening de sistemas, que consiste en remover servicios vulnerables e innecesarios, eliminar problemas de seguridad conocidos, configurar adecuadamente todos los dispositivos y asegurar los controles de acceso. Este proceso involucra realizar una evaluación y auditoría de la arquitectura de seguridad de la organización con el fin de desarrollar e implementar procedimientos de consolidación para asegurar sus recursos críticos. Estos procedimientos son personalizados, pero muchas de las tareas pueden automatizarse. Contar con herramientas adecuadas, que provean soporte al proceso de auditoría y faciliten la detección de las problemáticas se torna esencial. En este contexto, el Grupo de Seguridad Informática (GSI) de la Facultad de Ingeniería de la Universidad de la República (FING - UDELAR), ha realizado desde 2006 trabajo en torno al desarrollo de metodologías y herramientas

orientadas a la automatización de procedimientos y análisis de vulnerabilidades de seguridad informática. En Towards machine-assisted formal procedures for collection of digital evidence (Barrere, Betarte, Rodríguez, PST2011), se presenta un framework para la especificación de procedimientos de recolección de evidencia digital y se describe un prototipo de una herramienta para automatizar la ejecución de dichos procedimientos, basándose en una extensión, desarrollada por el equipo de investigación, de un lenguaje desarrollado por Mitre Corp, Open Vulnerability and Assessment Language (OVAL). OVAL forma parte de un conjunto de especificaciones que confluyen en el protocolo denominado Security Content Automation Protocol (SCAP). Dicho protocolo es propuesto y desarrollado por el Instituto Nacional de Estándares y Tecnología de Estados Unidos (NIST por sus siglas en inglés), y fue creado para proporcionar un enfoque estandarizado sobre el mantenimiento de la seguridad de los sistemas, incentivando la verificación y chequeo automático tanto de configuraciones erróneas o por defecto, análisis de vulnerabilidades y detección de compromisos de seguridad. El proyecto SATKit consiste en desarrollar una herramienta que provea soporte automatizado para realizar chequeos de configuraciones, seguridad y hardening de plataformas informáticas de las organizaciones utilizando la metodología y los estándares propuestos en SCAP. Además de las ventajas directas que ofrecerá contar con una herramienta de este tipo, pensamos que el desarrollo y uso de esta tecnología permitirá analizar nuevas tendencias tecnológicas en materia de seguridad informática, en particular aquellas orientadas a la consolidación de procedimientos que permitan asegurar los recursos críticos de una organización. Asimismo, pensamos que esta innovación creará bases para la conformación y desarrollo de grupos de trabajo que investiguen este tipo de estándares y tecnologías en el país, propiciando la creación y/o adaptación de normas técnicas a la realidad uruguaya, tanto en órganos de la administración del estado como en el sector privado.

6 horas semanales

Área de Consultoría Tecnológica, Equipo de Seguridad Informática

Desarrollo

Coordinador o Responsable

En Marcha

RRHH formados en el proyecto:

Especialización:1

Maestría/Magister:1

Equipo: R. MARTÍNEZ, M. RODRÍGUEZ

Palabras clave: Análisis de vulnerabilidades, soporte automatizado

Áreas de conocimiento:

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

#### **ModSecIntl: A machine learning-assisted web application firewall (10/2021 - 06/2023)**

El objetivo general de este proyecto es la concepción y desarrollo de mecanismos automatizados para la identificación, análisis y prevención de ataques informáticos a aplicaciones web. El resultado tecnológico del proyecto será un Producto Mínimo Viable (MVP) compuesto por modelos y herramientas que permitan dar soporte automatizado a estos mecanismos. Con el objetivo de mejorar la capacidad de detección y/o la reducción de falsos positivos del WAF ModSecurity hemos concebido un framework donde la idea principal es combinar la flexibilidad que proporcionan los procedimientos de clasificación obtenidos a partir de la definición de modelos de aprendizaje automático con el conocimiento codificado integrado en la especificación de las reglas que utiliza el WAF para detectar ataques. Un desafío importante es poder brindar la capacidad de integrar modelos de aprendizaje definidos por el usuario con el motor de decisión de reglas de ModSecurity. Este marco incorpora un entorno de desarrollo de modelos y un módulo clasificador llamado Web Attack Classification Engine (WACE).

6 horas semanales

Consultoría Tecnológica

Investigación

Coordinador o Responsable

Concluido

RRHH formados en el proyecto:

Pregrado:1

Financiación:

OEA, Estados Unidos, Apoyo financiero

Equipo: G. BETARTE, Rodrigo Martínez

Palabras clave: WAF Machine Learning Adaptive security

#### **WAFINTL: Un Framework de Ciber-seguridad para el Análisis y Prevención de Ataques en Aplicaciones Web (10/2015 - 07/2018)**

El drástico incremento de ataques informáticos obliga a los gobiernos, organizaciones y empresas, a considerar la seguridad de la información, de las aplicaciones y de la infraestructura informática como un tema prioritario. Una estrategia (defensiva) clave para garantizar el correcto aseguramiento y configuración de las aplicaciones informáticas incluye, entre otros, la utilización de técnicas de desarrollo seguro de código, testeos de seguridad de la aplicación y aseguramiento de la infraestructura sobre la que se ejecuta. Debido a la diversidad, multiplicidad y la continua innovación de los sistemas actuales se torna necesario automatizar procesos y generar herramientas que asistan a los desarrolladores, administradores de sistemas, auditores y analistas de seguridad en esta tarea. El proyecto WAFINTL tiene como objetivo general la concepción y desarrollo de mecanismos automatizados de identificación, así como el análisis y prevención de ataques informáticos de las aplicaciones web. También se enfoca en el desarrollo de procesos de ciber-inteligencia que provean soporte para el tratamiento sistematizado de las tareas de análisis. El resultado tecnológico del proyecto serán prototipos de herramientas que permitan dar soporte automatizado a esos mecanismos. Los objetivos específicos del proyecto son: - El desarrollo de técnicas de detección de ataques y determinación de perfiles de atacantes - Concepción, diseño e implementación de un honeypot de alto nivel de interacción para el registro y análisis de vectores de ataques - Concepción y desarrollo de herramientas para el soporte automatizado de técnicas de cyber threat intelligence

6 horas semanales

Investigación

Coordinador o Responsable

Concluido

RRHH formados en el proyecto:

Pregrado:1

Maestría/Magister:3

Financiación:

Agencia Nacional de Investigación e Innovación, Uruguay, Beca

Equipo: M. RODRÍGUEZ , E. GIMÉNEZ , R. MARTÍNEZ , A. PARDO

Palabras clave: Ciberinteligencia Aprendizaje automático Inferencia de conocimiento

Áreas de conocimiento:

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

#### **Plataforma de Control de Acceso a los recursos Internet del Plan Ceibal (04/2009 - 09/2015 )**

Para una fase avanzada de puesta en producción del Plan Ceibal, el LATU convocó a proceso licitatorio para la provisión de una solución que permita implementar control de acceso a los recursos que el estado uruguayo brindará a/en los establecimientos educativos del país, tales como acceso a Internet y portales educativos ad-hoc, con el objetivo de limitar de esta manera conexiones no autorizadas y la utilización indebida de dichos recursos. El Sistema de Control de Acceso (SCA) tiene como objetivo fundamental implementar el control de acceso a los servicios brindados por la Red Ceibal mediante uso de un Portal Cautivo para limitar conexiones no autorizadas y la utilización indebida de recursos. La Plataforma de Control de Acceso (PCA) esta especialmente diseñada para: 1) Realizar la autenticación de las laptops XO de forma automática y transparente, 2) Realizar autenticación mutua entre los clientes y los servidores de la PCA, 3) Permitir realizar la autenticación a usuarios del Plan Ceibal que cuenten con conectividad inalámbrica, y que puedan ingresar un usuario y clave (ej. Docentes y/o funcionarios) , 4) Ofrecer alta disponibilidad en todos sus servicios. Los componentes principales del proyecto son: 1) Análisis, diseño y construcción de un protocolo de autenticación, que permita la autenticación mutua y transparente, entre las XO y la PCA, 2) instalación y configuración de una plataforma centralizada, con distintas capas de aplicación (Front End , Servidores de aplicación, Back end) y zonas de seguridad, 3) construcción de una consola de administración Web, que permita gestionar el Sistema.

10 horas semanales

Área de Consultoría Tecnológica , Equipo de Seguridad Informática

Desarrollo

Coordinador o Responsable

Concluido

Equipo: M. RODRÍGUEZ , A. BLANCO , M. CANABÉ , LÓPEZ R./LÓPEZ CORREA R. , R. MARTÍNEZ , J.D. CAMPO , M. DEL RIEGO , F. ZIPITRÍA

Palabras clave: Control de acceso Plan ceibal

Áreas de conocimiento:

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

#### **DIRECCIÓN Y ADMINISTRACIÓN**

(03/2012 - a la fecha )

10 horas semanales

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

Facultad de Ingeniería / Instituto de Computación

#### VÍNCULOS CON LA INSTITUCIÓN

##### **Funcionario/Empleado (05/2010 - a la fecha)** Trabajo relevante

Profesor Titular 26 horas semanales

Desde que asumí este cargo he usufructuado extensiones a 30hs semanales que han sido financiadas con fondos extra presupuestales.

Escalafón: Docente

Grado: Grado 5

Cargo: Efectivo

##### **Otro (04/2010 - 12/2020)**

Investigador Activo Nivel I del SNI 26 horas semanales

Escalafón: Docente

Grado: Grado 5

Cargo: Efectivo

##### **Funcionario/Empleado (05/1998 - 04/2010)**

Profesor Agregado 30 horas semanales

Escalafón: Docente

Grado: Grado 4

Cargo: Efectivo

##### **Funcionario/Empleado (06/1990 - 04/1998)**

Asistente 40 horas semanales

Escalafón: Docente

Grado: Grado 2

Cargo: Interino

##### **Funcionario/Empleado (12/1986 - 05/1990)**

Ayudante 40 horas semanales

Escalafón: Docente

Grado: Grado 1

Cargo: Interino

#### ACTIVIDADES

##### PROYECTOS DE INVESTIGACIÓN Y DESARROLLO

##### **Herramientas conceptuales y tecnológicas para ciberseguridad adaptativa y certificada (03/2023 - a la fecha)**

El objetivo de este programa/ proyecto 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 a 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. También nos interesa diseñar y generar un prototipo funcional de un sistema, haciendo uso de tecnología blockchain, que brinde servicios para manejar, almacenar y validar certificados académicos digitales, que respete las regulaciones nacionales sobre el manejo de datos personales. En lo que respecta a la seguridad de aplicaciones web, se profundizará en el estudio de la aplicación de técnicas de aprendizaje automático y profundo y la seguridad guiada por modelos para incrementar la mejora en ejecución y

precisión de la detección de ataques de esetipo de aplicaciones. En particular nos focalizaremos en explorar el entrenamiento de modelos de aprendizaje usando solamente datos de ataques. Otro desafío importante es el de investigar la posibilidad de proponer una solución de inteligencia de amenazas, que incluya procesos de recolección, procesamiento, análisis y correlación de información, permitiendo, en base al conocimiento adquirido, la predicción o anticipación de ataques no registrados y clasificados (también conocidos como 0-day attacks). En cuanto a los entornos para entrenamiento en ciberseguridad, se trabajarán en la concepción, desarrollo e implementación de una nueva plataforma para entrenamientos en ciberseguridad, de tipo cyber range, que permita a los diferentes actores (docentes, entrenadores, estudiantes, profesionales e investigadores) definir, ejecutar, experimentar y resolver escenarios de ciberseguridad, así como administrar, generar reportes, y hacer el seguimiento de cursos y programas de entrenamiento. Estos escenarios permitirán, además de simular los sistemas tradicionales como, entre otros, servidores, routers y firewalls, generar prácticas para el estudio, por ejemplo, de tecnologías de video conferencia o dispositivos móviles, que han cobrado notoria relevancia en los últimos tiempos. De igual manera, un problema presente y que concita mucho interés (no solo de la comunidad académica) reside en el aseguramiento de la corrección y la seguridad de sistemas y protocolos de criptomonedas, dado que éstos constituyen software crítico que involucra importantes inversiones económicas. Formalizar y analizar sobre estos sistemas no solo propiedades de corrección sino también de seguridad resulta crucial.

10 horas semanales

Facultad de Ingeniería , Instituto de Computación

Investigación

Coordinador o Responsable

En Marcha

RRHH formados en el proyecto:

Pregrado:4

Maestría/Magister:2

Maestría/Magister prof:1

Doctorado:2

Financiación:

Comisión Sectorial de Investigación Científica, Uruguay, Apoyo financiero

Equipo: G. BETARTE , JUAN DIEGO CAMPO , LUNA, C.

Palabras clave: Ciberseguridad adaptativa Plataformas de entrenamiento Verificación de protocolos de criptomoneda

Areas de conocimiento:

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

### **Automatización de derivación de conocimiento para el aseguramiento de sistemas informáticos (03/2018 - 08/2021 )**

La actividad de investigación de 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. Con el objetivo de complementar y mejorar el desempeño de tecnologías de prevención de ataques como lo son los denominados firewall de aplicaciones (WAF por su sigla en inglés) se pretende desarrollar modelos y soluciones de aprendizaje automático para incrementar la mejora en ejecución y precisión de la detección de ataques por parte del WAF ModSecurity. Otro desafío importante que se plantea este proyecto es el de proponer una solución de ciberinteligencia que incluya procesos de recolección, procesamiento, análisis y correlación de información, permitiendo, en base al conocimiento adquirido, la predicción o anticipación de ataques no registrados y clasificados (también conocidos como 0-day attacks). Adicionalmente se explorará en mayor profundidad la aplicación de técnicas de seguridad guiada por modelos para la especificación de mecanismos que provean soporte automatizado para la aplicación de parches virtuales que permitan remediar vulnerabilidades de una aplicación sin que esto implique modificar el código de la misma. El resultado tecnológico del proyecto serán modelos y prototipos de herramientas que permitan dar soporte automatizado a esos mecanismos. Algunas de las principales características no funcionales que deben satisfacer las soluciones tecnológicas resultantes de este proyecto es que (i) estén basadas en estándares de código abierto de referencia para el mercado, (ii) no sean herramientas invasivas en lo que respecta a las aplicaciones web a proteger, (iii) ser flexibles y extensibles de forma de adaptarse a requerimientos en permanente evolución y (iv) ser independientes del sistema operativo sobre el que serán ejecutadas.

10 horas semanales

Universidad de la República , Facultad de Ingeniería

Investigación

Coordinador o Responsable

Concluido

RRHH formados en el proyecto:

Pregrado:5

Maestría/Magister:3

Financiación:

Agencia Nacional de Investigación e Innovación, Uruguay, Apoyo financiero

Equipo: G. BETARTE (Responsable) , ALVARO PARDO (Responsable) , LUNA, C. , JUAN DIEGO CAMPO , JUAN JOSÉ GOYENECHÉ

Palabras clave: Seguridad de Aplicaciones Aprendizaje Automático Minería de Datos Seguridad guiada por Modelos

Areas de conocimiento:

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

### **PROTECT (PRivacy Oriented TEchniques for the assessment of Contact Tracing solutions) (04/2020 - 11/2020)**

Al proyecto PROTECT lo conforma un equipo multi-disciplinario de docentes de la Universidad de la República cuyo trabajo se focaliza en investigar la problemática del uso de tecnologías digitales para implementar rastreo digital de proximidad con el objetivo de mejorar la eficacia del proceso de detección de contagios. En el contexto del proyecto PROTECT se ha trabajado, en primer lugar, en identificar las propuestas existentes, las tecnologías, flujos de datos y procesos involucrados en el funcionamiento de sistemas de Rastro Digital de Proximidad (RDP de aquí en más). Asimismo, se ha desarrollado un análisis preliminar de seguridad y privacidad de soluciones de RDP y los diferentes modelos definidos. Uruguay ha desplegado una solución tecnológica, usando una aplicación móvil, destinada a notificar a los usuarios si han estado en contacto con una persona diagnosticada con COVID-19. Con este trabajo se ha intentado contribuir aportando a identificar y definir con precisión, con la mirada puesta en la seguridad y la privacidad de las personas, lo que una aplicación de RDP como la CoronavirusUY podría, o no, garantizar al respecto.

10 horas semanales

Facultad de Ingeniería - UDELAR , Instituto de Computación

Otra

Coordinador o Responsable

Concluido

Equipo: Gustavo BETARTE GUIDI , Juan Diego CAMPO BARBÉ , A DELGADO , P. EZZATTI , Alvaro Javier FORTEZA GALCERÁN , L. GONZALEZ , Álvaro MARTÍN MENONI , B. MURACCIOLE , Raúl Julian RUGGIA FRICK

### **Mecanismos autónomos de seguridad certificados para sistemas computacionales móviles (10/2015 - 12/2018)**

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. Proyecto Fondo Clemente Estable - Edición 2014

10 horas semanales

Facultad de Ingeniería , Instituto de Computación

Investigación

Coordinador o Responsable

Concluido

RRHH formados en el proyecto:

Pregrado:7

Maestría/Magister:3

Financiación:

Agencia Nacional de Investigación e Innovación, Uruguay, Apoyo financiero  
Equipo: C. LUNA , J. BALIOSIAN , J. CAMPO , M. BARRERE  
Palabras clave: Dispositivos móviles Seguridad certificada Mecanismos autónomos  
Áreas de conocimiento:  
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Formal Methods, Security  
Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información / Ingeniería de Sistemas y Comunicaciones / Seguridad

**Autonomic Knowledge Discovery for Security Vulnerability Prevention in Self-governing Systems (AKD) (proyecto STIC Amsud 2014) (12/2014 - 12/2016)**

Hoy en día las vulnerabilidades informáticas constituyen uno de los principales puntos de entrada para los ataques de seguridad, y por lo tanto, los mecanismos de gestión de vulnerabilidad son cruciales para cualquier sistema computacional. Por otro lado, el paradigma de la informática autónoma está ganando cada vez más tracción como un nuevo modelo para gestionar sistemas y redes complejos. Hasta el momento las contribuciones se han ocupado de mecanismos autónomos para evaluar y remediar vulnerabilidades, sin embargo, estas soluciones son reactivas por naturaleza, y algunas veces corregir las vulnerabilidades de seguridad puede implicar actividades costosas que pueden degradar el rendimiento del sistema y eventualmente contradecir las políticas operacionales existentes. Este proyecto, en cambio, se ha orientado al diseño y desarrollo de un novedoso enfoque autónomo capaz de anticipar y prevenir futuros estados vulnerables. Para ello, un uso eficiente e inteligente del conocimiento administrado por entidades autónomas se vuelve esencial. El objetivo de la investigación es poder aprovechar este conocimiento utilizando principalmente un proceso de descubrimiento de conocimiento conceptual (CKDP), para integrar capacidades anticipatorias en el plano de la seguridad autónoma. CKDP es una extensión propuesta para el proceso estándar de descubrimiento de conocimiento con un núcleo conceptual que se apoya en las técnicas de Formal Concept Analysis (FCA). FCA se ha utilizado para diferentes aplicaciones de minería y gestión de conocimiento en múltiples subdominios de informática y bioinformática. El objetivo principal de este proyecto es el estudio de mecanismos de anticipación de vulnerabilidad desde la perspectiva de CKDP y FCA. Otro objetivo importante del proyecto es crear puentes entre dos dominios de investigación activos: la autonomía y el descubrimiento de conocimiento. Además, se apuntó a la integración de diferentes equipos con distintos enfoques de investigación. Tal trabajo de investigación puede sentar las bases para profundizar intercambio científico que involucra diferentes dominios de investigación tales como seguridad informática, inteligencia artificial, gestión de redes, métodos formales e ingeniería de software. En este proyecto han participado equipos de investigación de Brasil, Chile, Francia y Uruguay.

4 horas semanales

Facultad de Ingeniería , Instituto de Computación

Investigación

Coordinador o Responsable

Concluido

RRHH formados en el proyecto:

Pregrado:2

Maestría/Magister:1

Maestría/Magister prof:1

Financiación:

Agencia Nacional de Investigación e Innovación, Uruguay, Apoyo financiero

CNRS, Francia, Apoyo financiero

Institut National de Recherche en Informatique et Automatique, Francia, Apoyo financiero

Equipo: M. RODRÍGUEZ , M. BARRERE , J. BALIOSIAN

Palabras clave: Vulnerability management Knowledge discovery

Áreas de conocimiento:

Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información / Ingeniería de Sistemas y Comunicaciones / Análisis de vulnerabilidades, gestión autónoma de sistemas

**VirtualCert: Hacia una Plataforma de Virtualización Certificada - Fase II (03/2013 - 06/2015)**

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. Proyecto CSIC I+D - Edición 2012

15 horas semanales

Facultad de Ingeniería , Instituto de Computación

Investigación

Coordinador o Responsable

Concluido

RRHH formados en el proyecto:

Pregrado:2

Doctorado:2

Financiación:

Comisión Sectorial de Investigación Científica, Uruguay, Apoyo financiero

Equipo: C. LUNA , J.D. CAMPO , G. BARTHE

Palabras clave: Virtualización, No interferencia

Areas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Métodos formales, Seguridad

### **VirtualCert: Hacia una Plataforma de Virtualización Certificada (Proyecto Fondo Clemente Estable 2009) (01/2010 - 12/2012 )**

Este proyecto aborda el estudio del comportamiento de plataformas de computación virtuales. Específicamente, se focaliza en la especificación y verificación formal de determinadas propiedades de seguridad, que es deseable sean garantidas 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.

15 horas semanales

Facultad de Ingeniería , Instituto de Computación

Investigación

Coordinador o Responsable

Concluido

RRHH formados en el proyecto:

Pregrado:3

Maestría/Magister:1

Doctorado:2

Equipo: C. LUNA , J.D. CAMPO , G. BARTHE

Palabras clave: Virtualización, Seguridad, Formalización

Áreas de conocimiento:

Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información / Ingeniería de Sistemas y Comunicaciones / Seguridad Informática, Métodos Formales  
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Métodos Formales, Seguridad Informática

### **Sistema Unificado de Gestión de Identidad Electrónica (08/2011 - 09/2012)**

La AGESIC tiene como línea estratégica la realización de distintos proyectos e iniciativas con el objetivo de desarrollar una plataforma de gobierno electrónico en el Uruguay (e-government). Uno de los principales desafíos que la Agencia ha definido en su agenda es el de sentar las bases para desarrollar un Sistema Unificado de Gestión de Identificación Electrónica (Electronic Identity Management) de los ciudadanos o usuarios de la plataforma de gobierno electrónico (egovernment). Para impulsar estas líneas estratégicas y dar soporte informático a las necesidades que se presentan, AGESIC adquirió el sistema de gestión de Identificación Electrónica (eiManagement), TIVOLI Identity Management (TIM), de IBM. Asimismo, en forma paralela a esta iniciativa, AGESIC se encuentra en el proceso de despliegue de una infraestructura de clave pública o (Public Key Infrastructure - PKI) a nivel nacional, la cual estará operativa en la segunda mitad del 2011. Por otro lado, en forma complementaria a esta línea de investigación, se desea investigar el impacto en incorporar dispositivos portátiles que permitan almacenar y utilizar las credenciales y atributos que identifican a los ciudadanos y que aporten altos niveles de seguridad, bajo costo, fácil uso y la posibilidad de ser distribuido al conjunto de la población. A los efectos de desarrollar un sistema nacional de identificación electrónica del estado Uruguayo, y desarrollar estas líneas de investigación la AGESIC desea contar con el apoyo del Grupo de Seguridad Informática (GSI) de la Facultad de Ingeniería (FING) para el estudio de esta tecnología y el desarrollo de pruebas de concepto sobre la cual comenzar a desarrollar una prueba piloto de las mismas

4 horas semanales

Instituto de Computación, Grupo de Seguridad Informática

Investigación

Coordinador o Responsable

Concluido

RRHH formados en el proyecto:

Maestría/Magister prof:1

Doctorado:1

Equipo: D. PEDRAJA, GUSTAVO BETARTE (Responsable), P. LÓPEZ, M. E. CORTI, E. GIMÉNEZ, A. BLANCO, R. LÓPEZ

Palabras clave: Identidad electrónica, Seguridad

Áreas de conocimiento:

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

### **Actividad Específica nro. 3 "CERTuy" - convenio marco de investigación y desarrollo FING - ANTEL. (03/2006 - 12/2009)**

El principal objetivo de este proyecto es desarrollar actividades que contribuyan a la creación y formación de un CERT (Computer Emergency Response Team) nacional. Este proyecto está siendo desarrollado en colaboración con el CSIRT (Computer Security Incidents Response Team) de la compañía nacional de telecomunicaciones ANTEL.

6 horas semanales

Facultad de Ingeniería, Instituto de Computación

Extensión

Coordinador o Responsable

En Marcha

RRHH formados en el proyecto:

Pregrado:2

Maestría/Magister:4

Maestría/Magister prof:1

Doctorado:1

Equipo: WWW.FING.EDU.UY/INCO/GSI (Responsable)

Palabras clave: CERT, CSIRT, Seguridad

Áreas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Seguridad Informática

### **ReSeCo: Reliability and Security of Distributed Software Components. (12/2006 - 12/2009)**

El principal objetivo del proyecto ReSeCo es investigar la seguridad y fiabilidad en un modelo

computacional, donde tanto las plataformas como las aplicaciones son dinámicas, de forma que componentes provistos por un agente externo puedan ser destinados a formar parte de la plataforma o ejecutar una aplicación de forma segura. El proyecto tiene además como objetivo fundamental incentivar la colaboración entre la comunidad científica, e industrial, de Francia y de países Sudamericanos (Argentina, Chile y Uruguay).

6 horas semanales

Facultad de Ingeniería , Instituto de Computación

Investigación

Coordinador o Responsable

En Marcha

RRHH formados en el proyecto:

Maestría/Magister:1

Doctorado:1

Financiación:

Institución del exterior, Apoyo financiero

Equipo: WWW.FING.EDU.UY/INCO/GRUPOS/MF (Responsable)

Palabras clave: Métodos Formales, Seguridad de Software

Areas de conocimiento:

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

Computación / Métodos Formales, Seguridad Informática

### **STEVE: Seguridad a Través de Evidencia Verificable (02/2007 - 03/2009 )**

El principal objetivo del proyecto STEVE es investigar la seguridad y fiabilidad en un modelo computacional, donde tanto las plataformas como las aplicaciones son dinámicas, de forma que componentes provistos por un agente externo puedan ser destinados a formar parte de la plataforma o ejecutar una aplicación de forma segura. Este es un proyecto PDT de Investigación Fundamental.

10 horas semanales

Facultad de Ingeniería , Instituto de Computación

Investigación

Coordinador o Responsable

En Marcha

RRHH formados en el proyecto:

Especialización:1

Maestría/Magister:1

Equipo: WWW.FING.EDU.UY/INCO/GRUPOS/MF (Responsable)

Palabras clave: Métodos Formales, Seguridad de Software

Areas de conocimiento:

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

Computación / Métodos Formales, Seguridad Informática

### **Projet de Collaboration Régionale Côte-Sud France: Cartes à Puce. (07/2001 - 07/2002 )**

Este es un proyecto de investigación en el dominio de Tarjetas Inteligentes en el que colaboraron equipos de INRIA Sophia-Antipolis, Francia, Universidad de Córdoba, Argentina e InCo, Uruguay. Este proyecto fue parcialmente financiado por el gobierno Francés.

10 horas semanales

Facultad de Ingeniería , Instituto de Computación

Investigación

Coordinador o Responsable

Concluido

RRHH formados en el proyecto:

Pregrado:1

Maestría/Magister:1

Financiación:

Institución del exterior, Apoyo financiero

Equipo: WWW.FING.EDU.UY/INCO/GRUPOS/MF (Responsable)

Palabras clave: Métodos Formales, Tarjetas Inteligentes

Areas de conocimiento:

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

Computación / Métodos Formales, Seguridad Informática

### **Integración de Teoría de Tipos y Verificación de Modelos para la Certificación Formal de Sistemas Reactivos (03/2000 - 03/2002 )**

Este proyecto tuvo como objetivo principal el desarrollar investigación orientada a la integración

del usos de asistentes de pruebas basados en la teoría constructiva de tipos y herramientas de verificación de modelos en la obtención de especificaciones certificadas de sistemas críticos.

15 horas semanales

Facultad de Ingeniería , Instituto de Computación

Investigación

Coordinador o Responsable

Concluido

RRHH formados en el proyecto:

Maestría/Magister:1

Doctorado:1

Financiación:

Comisión Sectorial de Investigación Científica, Uruguay, Apoyo financiero

Equipo: WWW.FING.EDU.UY/INCO/MF (Responsable)

Palabras clave: Teoría de Tipos, Model checking

Areas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Teoría de Tipos

### **Subtipos y Objetos en teorías y herramientas de programación basadas en Teoría de Tipos (05/1999 - 03/2001)**

La investigación propuesta en este proyecto tiene su origen en la teoría de tipos con record types y subtipado formulada en las tesis doctoral de Alvaro Tasistro, que es a su vez una extensión de la Teoría de Tipos de Martin-Loef. Consiste en el desarrollo de los siguientes temas: inclusión de tipos, modelos formales de la programación orientada a objetos e implementación de asistentes de desarrollo de derivaciones formales. El objetivo final es llevar a la práctica métodos de desarrollo de programas de corrección certificada. En este plano, el punto de partida es un prototipo, presentado en la tesis doctoral de Gustavo Betarte, que se basa en la extensión de la teoría constructiva de tipos citada al comienzo.

10 horas semanales

Facultad de Ingeniería , Instituto de Computación

Investigación

Integrante del Equipo

Concluido

Equipo: WWW.FING.EDU.UY/INCO/GRUPOS/MF

Palabras clave: Teoría de Tipos, Subtipado

Areas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Teoría de Tipos, Objetos

## **DOCENCIA**

### **Maestría en Ingeniería (Ingeniería en Computación) (04/2010 - a la fecha)**

Maestría

Responsable

Asignaturas:

Seguridad de Sistemas, 6 horas, Teórico-Práctico

Seguridad en Aplicaciones, 5 horas, Teórico-Práctico

Gestión de la Seguridad de la Información, 6 horas, Teórico-Práctico

Areas de conocimiento:

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

### **Ingeniería en Computacion (09/2010 - a la fecha)**

Grado

Responsable

Asignaturas:

Taller de Seguridad Informática, 4 horas, Teórico-Práctico

Areas de conocimiento:

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

### **Ingeniería en Computación (09/2005 - a la fecha)**

Grado

Responsable

Asignaturas:

Construcción Formas de Programas en Teoría de Tipos, 12 horas, Teórico-Práctico

Áreas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Teoría de Tipos, Logical Frameworks

**Ingeniería en Computación (04/2007 - a la fecha)**

Grado

Responsable

Asignaturas:

Fundamentos de la Seguridad Informática, 10 horas, Teórico-Práctico

Áreas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Seguridad Informática

**Diploma en la Especialización Estudios Avanzados en Computación (08/2014 - a la fecha)**

Especialización

Responsable

Asignaturas:

Metodologías para el Análisis Forense Informático, 6 horas, Teórico-Práctico

Áreas de conocimiento:

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

**Ingeniería en Computación (08/2020 - a la fecha)**

Grado

Asistente

Asignaturas:

Computación 1, 8 horas, Teórico-Práctico

**Escuela Latinoamericana de Informática (08/2024 - 08/2024 )**

Especialización

Responsable

Asignaturas:

Análisis forense digital y respuesta a incidentes: un enfoque práctico, 30 horas, Teórico-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 (07/2019 - 07/2020 )**

Grado

Asistente

Asignaturas:

Programación 1, 10 horas, Teórico-Práctico

**Ingeniería en Computación (03/1999 - 07/2000 )**

Grado

Asignaturas:

Programación 2, 10 horas, Teórico-Práctico

Áreas de conocimiento:

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

**Ingeniería en Computación (03/1997 - 07/1997 )**

Grado

Asignaturas:

Programación 1, 10 horas, Teórico-Práctico

**Ingeniería en Computación (08/1991 - 12/1991 )**

Grado

Asignaturas:  
Teoría de la Programación 2, 10 horas, Teórico

**Ingeniería en Computación (03/1990 - 07/1990 )**

Grado

Asignaturas:  
Organización de Lenguajes de Programación, 10 horas, Teórico

**Ingeniería en Computación (08/1987 - 12/1988 )**

Grado

Asignaturas:  
Programación 2, 10 horas, Teórico-Práctico

**EXTENSIÓN**

**(03/2006 - a la fecha )**

Facultad de Ingeniería, Instituto de Computación  
6 horas

Areas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Seguridad Informática

**SERVICIO TÉCNICO ESPECIALIZADO**

**(05/2016 - 09/2016 )**

Facultad de Ingeniería, Instituto de Computación  
2 horas semanales

**(09/2015 - 05/2016 )**

Facultad de Ingeniería, Instituto de Computación  
2 horas semanales

**(04/2015 - 09/2015 )**

Facultad de Ingeniería, Instituto de Computación  
2 horas semanales

**GESTIÓN ACADÉMICA**

**Responsable del Grupo de Seguridad Informática de FING (03/2006 - a la fecha )**

Facultad de Ingeniería, Instituto de Computación  
Gestión de la Investigación

Areas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Seguridad Informática

**Integrante de comisiones asesoras y tribunales en concursos para proveer cargos de Profesor Titular (Gr. 5), Profesor Agregado (Gr. 4), Profesor Adjunto (Gr. 3) y Asistente (Gr. 2) del Instituto de Computación de la Facultad de Ingeniería, UDELAR. (05/1998 - a la fecha )**

Facultad de Ingeniería, Instituto de Computación  
Participación en consejos y comisiones

**Responsable académico del Diploma de Especialización en Seguridad Informática (03/2012 - a la fecha )**

Instituto de Computación, Centro de Posgrados y Actualización Profesional (CPAP)  
Participación en consejos y comisiones

**Responsable y Coordinador de la Maestría en Seguridad Informática (01/2015 - a la fecha )**

Facultad de Ingeniería, Instituto de Computación  
Gestión de la Enseñanza  
Areas de conocimiento:

**Representante de la Universidad de la República en el Consejo Asesor Honorario de Seguridad Informática de la AGESIC (03/2008 - 03/2010)**

Facultad de Ingeniería, Instituto de Computación

Participación en consejos y comisiones

Áreas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Seguridad Informática

**Asistente Académico de Informática (05/2005 - 05/2007)**

Facultad de Ingeniería, Instituto de Computación

Otros

**Responsable científico del Laboratorio de Ciencia de la Computación y del Grupo de Métodos Formales (09/1999 - 03/2001)**

Facultad de Ingeniería, Instituto de Computación

Gestión de la Investigación

Áreas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Teoría de Tipos, Logical Frameworks, Métodos formales

**Integrante de la Comisión de Ciencias Básicas (06/1998 - 03/2001)**

Facultad de Ingeniería, Instituto de Computación

Participación en consejos y comisiones

Áreas de conocimiento:

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

**CARGA HORARIA**

Carga horaria de docencia: 8 horas

Carga horaria de investigación: 12 horas

Carga horaria de formación RRHH: 6 horas

Carga horaria de extensión: 2 horas

Carga horaria de gestión: 2 horas

## Producción científica/tecnológica

Soy el responsable del Grupo de Seguridad Informática ([GSI](#)) de la Facultad de Ingeniería de la Universidad de la República y el responsable científico e investigador principal del programa de investigación Herramientas conceptuales y tecnológicas para ciberseguridad adaptativa y certificada, presentado al llamado Grupos I+D de CSIC-Udelar, edición 2022, que fue seleccionado para recibir apoyo económico.

Mi actividad de investigación reciente concierne dos disciplinas de la Ciencia y la Ingeniería de la Computación: Métodos Formales y Seguridad Informática. En los últimos cuatro años la actividad de investigación y desarrollo realizada ha estado focalizada en tres líneas de actividad específicas:

Modelado, verificación formal y testing de mecanismos de seguridad de plataformas computacionales críticas.

Desarrollo y aplicación de técnicas de machine learning, deep learning, process mining y model-driven security para el aseguramiento de aplicaciones web y el perfilado de atacantes.

Concepción, diseño e implementación de plataformas de entrenamiento en ciberseguridad.

En lo que concierne a la primera línea de actividad, hemos investigado la aplicación de técnicas de proof-checking y model-based testing para la verificación de corrección de protocolos de criptomonedas. El entendimiento, modelado e implementación de mecanismos de verificación y refinamiento de contratos inteligentes correctos y seguros constituye un desafío de interés científico que ha sido muy tímidamente abordado en forma sistemática y haciendo uso de herramientas de especificación y verificación formal. Esta línea de investigación dio lugar al desarrollo de una tesis de maestría que ha sido premiada en concursos regionales y nacionales.

En lo que respecta a la seguridad de aplicaciones web, estamos investigando la aplicabilidad y adaptación de técnicas de detección de anomalías y de aplicación de modelos estadísticos en el

contexto de detección y prevención de ataques a aplicaciones web. Junto con mi equipo de investigación y en colaboración con otros investigadores nos estamos focalizando en el desarrollo de técnicas de detección de ataques y determinación de perfiles de atacantes usando técnicas de aprendizaje automático y minería de procesos así como en la concepción y desarrollo de herramientas para el soporte automatizado de técnicas de inteligencia de ciberamenazas. Ya contamos con resultados sumamente auspiciosos, obtenidos en el marco de dos proyectos de investigación y de dos trabajos de tesis de maestría supervisadas por quien suscribe y que fueron exitosamente defendidas. Una tesis de doctorado esta siendo desarrollada actualmente en esta línea de investigación. Una descripción detallada de los proyectos desarrollados y los resultados obtenidos se provee en [WAFMind](#).

Asimismo, hemos explorado un enfoque para modelar el comportamiento de atacantes basado en la aplicación de técnicas de minería de procesos y haciendo uso de la taxonomía MITRE ATT&CK. Dicho enfoque consta de cuatro pasos que siguen una metodología de minería de procesos estándar: 1) ejecutar estrategias de ataque dentro del sistema de software objetivo, 2) los datos se extraen, integran y cargan para crear registros de eventos, que sirven como fuente principal de información para el análisis. Estos registros se clasifican y etiquetan utilizando la taxonomía MITRE ATT&CK, 3) esta fase se centra en descubrir un modelo de proceso que represente el comportamiento de los atacantes a través de algoritmos de descubrimiento de procesos. Finalmente, 4) se interpretan y evalúan los resultados del modelo generado. Ya tenemos un artículo aceptado en una conferencia internacional arbitrada y otro publicado en una revista arbitrada regional de nivel Q2.

En lo que concierne a la tercera línea de actividad, y junto a miembros del equipo de investigación que lidero ([GSI](#)), hemos años diseñado e implementado Tectonic, una plataforma de entrenamiento en ciberseguridad (cyber range) que utiliza tecnologías de virtualización y nube de última generación. La plataforma ofrece un entorno de formación en el que los estudiantes universitarios pueden complementar, mediante ejercicios prácticos, los conocimientos teóricos adquiridos en diversas carreras de pregrado y posgrado en materia de ciberseguridad. Tectonic incorpora un lenguaje de especificación de escenarios que agiliza el proceso de definición y ejecución de escenarios para los docentes. Esta funcionalidad también facilita y fomenta la compartición de escenarios entre diversas instituciones. Además, la plataforma ofrece una variedad de funciones para evaluar el progreso de la formación de los estudiantes mediante el análisis de sus actividades registradas durante la formación. Esto permite a los docentes comprender mejor las tareas que realizan los estudiantes para lograr los objetivos de la formación. Ya tenemos 2 artículos aceptados en conferencias arbitradas. Información detallada sobre esta tecnología y acceso a su código está disponible en [Tectonic](#).

El trabajo de investigación desarrollado en estos últimos 5 años ha dado lugar a la publicación de 8 (ocho) artículos en revistas arbitradas, 12 (doce) artículos en conferencias internacionales arbitradas y 5 (cinco) pre-prints ([DBLP](#)). Desde 2019 mis publicaciones han recibido 491 referencias ([SCHOLAR](#)).

En el periodo reportado fui director de tesis de 2 tesis de maestría del Pedeciba Informática ([1er premio de CLTM 2022 y 2do premio del CLTM 2023](#) y [premio Pedeciba Informática 2022](#)), 1 tesis de maestría del programa de Ingeniería Matemática y 1 tesis de maestría en Computación de FING-Udelar. Actualmente soy el director académico y de tesis de 1 tesis de doctorado y director de tesis de 2 tesis de maestría del mismo programa.

Soy miembro fundador de la red [CiberLac](#), red de excelencia académica en ciberseguridad para Latinoamérica y el Caribe, creada en diciembre de 2021. Esta red está integrada por 30 universidades e institutos de investigación de la región y la Red Académica Nacional Brasileira (RNP). Fui el presidente de CiberLac desde junio de 2022 a junio de 2024. En 2023 y 2024 lideré el equipo de organización de las dos instancias del workshop Hacia una visión integrada y transversal del estado de la Ciberseguridad en América Latina y el Caribe, realizado en el marco de las conferencias [CLEI 2023](#) y [CLEI 2024](#).

Desde mayo 2020 a junio 2021 integré el Grupo Científico Asesor Honorario Nacional ([GACH](#)), contribuyendo a proveer asesoramiento científico al gobierno uruguayo en el área de modelos y ciencia de datos a través del equipo de gobierno Transición UY de COVID-19. Junto con miembros de mi equipo de investigación realizamos el análisis de seguridad y protección de datos personales de la aplicación [Coronavirus UY](#).

## Producción bibliográfica

### ARTÍCULOS PUBLICADOS

#### ARBITRADOS

##### **Assessment of Red and Blue Team Training in the Cyber Range Tectonic using Process Mining (Completo, 2025)**

GUILLERMO GUERRERO , GUSTAVO BETARTE , JUAN DIEGO CAMPO  
CLEI Electronic Journal, v.: 28 2025

Palabras clave: Red and Blue Team Tectonic Process mining

Escrito por invitación

E-ISSN: 07175000

DOI: [10.19153/cleiej.28.5.2](https://doi.org/10.19153/cleiej.28.5.2)

<https://doi.org/10.19153/cleiej.28.5.2>



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

NICOLÁS SERRANO , GUSTAVO BETARTE , JUAN DIEGO CAMPO

Journal of Internet Services and Applications, v.: 15 p.:139 - 159, 2024

Palabras clave: COVID-19 Trackers Data privacy

Areas 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

Escrito por invitación

ISSN: 18674828

E-ISSN: 18690238

DOI: [10.5753/jisa.2024.3882](http://dx.doi.org/10.5753/jisa.2024.3882)

<http://dx.doi.org/10.5753/jisa.2024.3882>



##### **A process mining-based method for attacker profiling using the MITRE ATT&CK taxonomy (Completo, 2024)**

MARCELO RODRÍGUEZ , GUSTAVO BETARTE , DANIEL CALEGARI

Journal of Internet Services and Applications, v.: 15 p.:212 - 232, 2024

Palabras clave: Attacker profile Process mining MITRE ATT&CK

Areas 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

Escrito por invitación

ISSN: 18674828

E-ISSN: 18690238

DOI: [10.5753/jisa.2024.3902](http://dx.doi.org/10.5753/jisa.2024.3902)

<http://dx.doi.org/10.5753/jisa.2024.3902>



##### **A Formal Analysis of the Mimblewimble Cryptocurrency Protocol with a Security Approach (Completo, 2024)**

ADRIAN SILVEIRA , GUSTAVO BETARTE , CARLOS LUNA

CLEI Electronic Journal, v.: 27 2024

Palabras clave: Mimblewimble Cryptocurrency Protocol Security

Areas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Lógica de la Programación, Métodos Formales, Seguridad Informática

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

Medio de divulgación: Internet

Escrito por invitación  
E-ISSN: 07175000  
DOI: [10.19153/cleiej.27.3.4](https://doi.org/10.19153/cleiej.27.3.4)  
<http://dx.doi.org/10.19153/cleiej.27.3.4>



**A Methodological Approach for the Security Analysis of FIWARE Technology (Completo, 2024)**

JUAN PABLO PERATA , GUSTAVO BETARTE  
CLEI Electronic Journal, v.: 27 2024  
Palabras clave: FIWARE security assessment threat analysis  
Areas 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  
Escrito por invitación  
E-ISSN: 07175000  
DOI: [10.19153/cleiej.27.4.2](https://doi.org/10.19153/cleiej.27.4.2)  
<http://dx.doi.org/10.19153/cleiej.27.4.2>



**A Blockchain based and GDPR-compliant design of a system for digital education certificates (Completo, 2023)**

G. BETARTE , LUNA, C. , F. Molina  
CLEI Electronic Journal, 2023  
Palabras clave: Blockchain Off-chain GDPR personal data protection laws design principles security and privacy threat analysis  
Medio de divulgación: Internet  
E-ISSN: 07175000  
DOI: <https://doi.org/10.19153/cleiej.26.1.3>



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

G. BETARTE , J. CAMPO , A. DELGADO , L. GONZALEZ , A. MARTIN , R. MARTINEZ , B. MURACCIOLE  
CLEI Electronic Journal, v.: 25 2 , p.:1 - 21, 2022  
Palabras clave: COVID-19 digital contact tracing security privacy protocols  
Areas 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  
Escrito por invitación  
E-ISSN: 07175000  
DOI: <https://doi.org/10.19153/cleiej.25.2.4>  
<http://www.clei.org/cleiej/index.php/cleiej/article/view/537>



**Set-Based Models for Cryptocurrency Software (Completo, 2021)**

GUSTAVO BETARTE , MAXIMILIANO CRISTIÁ , CARLOS LUNA , ADRIÁN SILVEIRA , DANTE ZANARINI  
CLEI Electronic Journal, v.: 24 3 , 2021  
Palabras clave: Cryptocurrency protocols MibleWimble Verification  
Areas de conocimiento:  
Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información / Seguridad Informática, Métodos Formales  
Medio de divulgación: Internet  
E-ISSN: 07175000  
DOI: [10.19153/cleiej.24.3.0](https://doi.org/10.19153/cleiej.24.3.0)  
<http://dx.doi.org/10.19153/cleiej.24.3.0>



### **A Formal Analysis of the Mimblewimble Cryptocurrency Protocol (Completo, 2021)**

ADRIÁN SILVEIRA, GUSTAVO BETARTE, MAXIMILIANO CRISTIÁ, CARLOS LUNA

Sensors, v.: 21 p.:5951 2021

Palabras clave: cryptocurrency; mimblewimble; idealized model; formal verification; security

Medio de divulgación: Internet

Lugar de publicación: Switzerland

E-ISSN: 14248220

DOI: [10.3390/s21175951](https://doi.org/10.3390/s21175951)

<http://dx.doi.org/10.3390/s21175951>

WEB OF SCIENCE™ Scopus®

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

G. BETARTE, G. Barthe, JUAN DIEGO CAMPO, LUNA, C., D. Pichardie

Journal of Automated Reasoning, 2020

Áreas de conocimiento:

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

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Seguridad Informática

Medio de divulgación: Internet

ISSN: 01687433

E-ISSN: 15730670

DOI: [10.1007/s10817-020-09548-x](https://doi.org/10.1007/s10817-020-09548-x)

<https://link.springer.com/article/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

G. BARTHE, G. BETARTE, J.D. CAMPO, C. LUNA

Journal of Automated Reasoning, v.: 63 p.:1 - 51, 2019

Palabras clave: Non-interference Cryptography Idealized model

Áreas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Formal Methods, Security

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

Medio de divulgación: Internet

E-ISSN: 15730670

DOI: [10.1007/s10817-017-9441-5](https://doi.org/10.1007/s10817-017-9441-5)

<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)**

G. BETARTE, JUAN DIEGO CAMPO, M. CRISTIA, F. GOROSTIAGA, LUNA, C., C. Sanz

Clei Electronic Journal, v.: 12, 2018

Palabras clave: Formal verification Security model Android

Áreas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Formal Methods, Computer Security

Medio de divulgación: Internet

Escrito por invitación

ISSN: 7175000

DOI: <https://doi.org/10.19153/cleiej.21.2>

<http://www.clei.org/cleiej/index.php/cleiej/article/view/41>


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

G. BETARTE, J. CAMPO, F. GOROSTIAGA, C. LUNA

Scientific Annals of Computer Science, v.: XXVI 2016

Palabras clave: Android Formal analysis Security model

Áreas de conocimiento:


Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Seguridad Informática, Métodos Formales  
Medio de divulgación: Internet  
Escrito por invitación  
ISSN: 18438121  
E-ISSN: 22482695  


**Formal Analysis of Security Models for Mobile Devices, Virtualization Platforms, and Domain Name Systems (Completo, 2015)**


G. BETARTE , C. LUNA  
CLEI Electronic Journal, 2015  
Palabras clave: Security Formal Methods  
Areas de conocimiento:  
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Seguridad Informática, Métodos Formales  
Medio de divulgación: Internet  
E-ISSN: 07175000



**A Formal Specification of the DNSSEC Model (Completo, 2012)**

EZEQUIEL BAZÁN , G. BETARTE , C. LUNA  
Electronic Communications of the EASST, 2012  
Palabras clave: DNSSEC Modelo formal verificado  
Areas de conocimiento:  
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Seguridad, Métodos Formales  
Medio de divulgación: Internet  
Lugar de publicación: Berlín  
E-ISSN: 18632122  
<http://journal.ub.tu-berlin.de/index.php/eceasst/index>  


**ACTkit: A Framework for the Definition and Enforcement of Role, Content and Context-based Access Control Policies (Completo, 2012)**

G. BETARTE , A. GATTO , R. MARTÍNEZ , F. ZIPITRÍA  
IEEE Latin America Transactions, v.: 10 3 , p.:1742 - 1751, 2012  
Palabras clave: RBAC, context and content-based access control  
Areas de conocimiento:  
Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información / Ingeniería de Sistemas y Comunicaciones / Seguridad  
Medio de divulgación: Internet  
E-ISSN: 15480992  


**Type Checking Dependent (record) Types and Subtyping (Completo, 2000) **

G. BETARTE  
Journal of Functional Programming, v.: 10 2 , p.:137 - 166, 2000  
Palabras clave: Type theory, Dependent record types  
Areas de conocimiento:  
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Type Theory, Logical frameworks  
Medio de divulgación: Internet  
Lugar de publicación: Cambridge University Press  
ISSN: 09567968  
E-ISSN: 14697653  
DOI: [10.1017/S0956796899003627](https://doi.org/10.1017/S0956796899003627)



**LIBROS**

**Actas del V Congreso Iberoamericano de Seguridad Informática ( Compilación , 2009) **

G. BETARTE , J. RAMIÓ AGUIRRE , A. RIBAGORDA GARNACHO

Número de volúmenes: 1

Número de páginas: 546

Edición: 1 , Montevideo

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

Medio de divulgación: CD-Rom

ISSN/ISBN: 9974005938

Financiación/Cooperación:

Agencia Nacional de Investigación e Innovación / Apoyo financiero, Uruguay

Comisión Sectorial de Investigación Científica / Apoyo financiero, Uruguay

Facultad de Ingeniería - UDeLaR / Cooperación, Uruguay

Programa de Desarrollo de las Ciencias Básicas / Cooperación, Uruguay

<http://www.fing.edu.uy/inco/eventos/cibsi09/Actas>

**Aportes al PENCTI: Tecnologías de la Información y Comunicación ( Completo , 2008)** Publicado

G. BETARTE , CANCELTA, H. , MOLERI, J.

Palabras clave: PENCTI, TIC

Areas de conocimiento:

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

Medio de divulgación: Papel

ISSN/ISBN: 9974816664

[http://www.anii.org.uy/imagenes/libro\\_tic.pdf](http://www.anii.org.uy/imagenes/libro_tic.pdf)

**Twenty-Five Years of Constructive Type Theory ( Participación , 2000)** Publicado Trabajo relevante

G. BETARTE , A. TASISTRO

Editor/Compilador: Giovanni Sambini, Jan M. Smith

Editorial: Oxford Science Publications , Oxford

Palabras clave: Type theory, dependent record types, subtyping

Areas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Type Theory, Logical frameworks

Medio de divulgación: Papel

ISSN/ISBN: 0198501277

Capítulos:

Extension of Martin-Löf's Type Theory with Record Types and Subtyping

Página inicial 21, Página final 39

**DOCUMENTOS DE TRABAJO**

**Capturing the security expert knowledge in feature selection for web application attack detection (2024)**

Completo

G. BETARTE , ALVARO PARDO

Palabras clave: Feature selection Expert knowledge Attack detection

Areas 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

<https://arxiv.org/abs/2407.18445>

**A Formal Analysis of the MimbleWimble Cryptocurrency Protocol (2021)**

Completo

G. BETARTE , ADRIAN SILVEIRA ABERASTURY , LUNA, C.

Medio de divulgación: Internet

<https://arxiv.org/abs/2104.00822>

**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 , ALVARO FORTEZA , L. GONZALEZ , ÁLVARO MARTÍN , B. MURACCIOLE , RUGGIA, R.

Palabras clave: Rastreo digital de proximidad Análisis de riesgos

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

<https://www.fing.edu.uy/inco/proyectos/protect/>

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

Completo

G. BETARTE , JUAN DIEGO CAMPO , A. DELGADO , P. EZZATTI , ALVARO FORTEZA , L. GONZALEZ , ÁLVARO MARTÍN , B. MURACCIOLE , RUGGIA, R.

Palabras clave: Rastreo digital de proximidad Privacidad y seguridad análisis de riesgos

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

<https://www.fing.edu.uy/inco/proyectos/protect/>

**A Blockchain based and GDPR-compliant design of a system for digital education certificates (2020)**

Completo

G. BETARTE , LUNA, C., F. Molina

arXiv:2010.12980

Palabras clave: Blockchain GDPR Privacy

Áreas de conocimiento:

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

Medio de divulgación: Internet

<https://arxiv.org/abs/2010.12980>

**Towards a formally verified implementation of the MimbleWimble cryptocurrency protocol (2019)**

Completo

G. BETARTE , M. CRISTIA , A. SILVEIRA , D. ZANARINI

arXiv:1907.01688

Palabras clave: Cryptocurrency MimbleWimble Formal verification

Áreas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Formal Methods, Computer Security

Medio de divulgación: Internet

<https://arxiv.org/abs/1907.01688>

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

Completo

G. BETARTE , C. LUNA , M. CHIMENTO

Serie: 0797-6410, v: 212

Palabras clave: Modelos memoria Virtualización

Áreas de conocimiento:

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

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

G. BETARTE , A. BLANCO , J.D. CAMPO , M. E. CORTI , C. LUNA , M. RODRÍGUEZ , F. ZIPITRÍA  
Serie: 0797-6410, v: 910  
Montevideo, Uruguay  
Palabras clave: Seguridad Informática UdelaR  
Areas de conocimiento:  
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Seguridad  
Medio de divulgación: Internet  
<http://www.fing.edu.uy/inco/pedeciba/bibpm/field.php/Main/ReportesT%e9cnicos>

**A formal specification and analysis of access control models for interactive mobile devices (2008)**

Completo  
G. BETARTE , J. M. CRESPO , C. LUNA  
Serie: 0797-6410, v: 807  
Montevideo, Uruguay  
Palabras clave: Access Control, Mobile Devices, Formal Framework  
Areas de conocimiento:  
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Métodos Formales y Seguridad  
Medio de divulgación: Internet  
<http://www.fing.edu.uy/inco/pedeciba/bibliote/reptec/TR0807.pdf>

**Hacia una especificación formal del modelo de seguridad de MIDP 3.0 (2008)**

Completo  
G. BETARTE , C. LUNA , G. MAZEIKIS  
Serie: 0797-6410, v: 808  
Montevideo, Uruguay  
Palabras clave: Access Control, Mobile Devices, Formal Framework  
Areas de conocimiento:  
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Métodos Formales y Seguridad  
Medio de divulgación: Internet  
<http://www.fing.edu.uy/inco/pedeciba/bibliote/reptec/TR0808.pdf>

**A Certified Access Controller for JME-MIDP 2.0 enabled Mobile Devices (2008)**

Completo  
G. BETARTE , C. LUNA , R. ROUSHANI  
Serie: 0797-6410, v: 608  
Montevideo, Uruguay  
Palabras clave: Access controller, MIDP 2.0  
Areas de conocimiento:  
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Métodos Formales y Seguridad  
Medio de divulgación: Internet  
<http://www.fing.edu.uy/inco/pedeciba/bibpm/field.php/Main/ReportesT%e9cnicos>

**Especificación y verificación formal de sistemas críticos en el Instituto de Computación de la Universidad de la República (2007)**

Completo  
G. BETARTE , C. LUNA , L. SIERRA  
Serie: 0797-6410, v: 714  
Palabras clave: Métodos Formales, Sistemas críticos  
Areas de conocimiento:  
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Métodos Formales y Seguridad  
Medio de divulgación: Internet

**A Formal Specification of the MIDP 2.0 Security Model (2006)**

Completo  
G. BETARTE , C. LUNA , S. ZANELLA  
Serie: 0797-6410, v: 609  
Palabras clave: Formal model and proofs MIDP 2.0  
Areas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Métodos Formales y Seguridad  
Medio de divulgación: Internet

**Proof reutilization in Martin-Löf's logical framework extended with record types and subtyping (2000)**

Completo  
G. BETARTE  
Serie: 0797-6410,  
Montevideo, Uruguay  
Palabras clave: Proof reutilisation, dependent record types  
Areas de conocimiento:  
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Métodos Formales, Type Theory  
Medio de divulgación: Internet

**Experiences with a Mechanisation of Martin-Löf's theory of types (1992)**

Completo  
G. BETARTE , E. GIMÉNEZ  
Serie: 0797-6410,  
Montevideo, Uruguay  
Palabras clave: Theory of Types, Logical Frameworks  
Areas de conocimiento:  
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Métodos Formales, Type Theory  
Medio de divulgación: Internet

**PUBLICACIÓN DE TRABAJOS PRESENTADOS EN EVENTOS**

**A comparative study of implementations for validating consent in personal data access control (2025)**

MARÍA FERNANDA MOLINA , GUSTAVO BETARTE , CARLOS LUNA  
Publicado  
Completo  
Descripción: 2025 LI Latin American Computer Conference (CLEI)  
Ciudad: Valparaíso, Chile  
Año del evento: 2025  
Anales/Proceedings: 2025 LI Latin American Computer Conference (CLEI)  
ISSN/ISBN: 979-8-3315-9453-4  
Publicación arbitrada  
Editorial: IEEE  
Palabras clave: Consent validation Personal data access control  
Areas 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  
DOI: [10.1109/clei67442.2025.11420618](https://doi.org/10.1109/clei67442.2025.11420618)  
Financiación/Cooperación:  
Comisión Sectorial de Investigación Científica / Apoyo financiero, Uruguay  
<https://doi.org/10.1109/clei67442.2025.11420618>

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

GUILLERMO GUERRERO , GUSTAVO BETARTE , JUAN DIEGO CAMPO  
Publicado  
Completo  
Evento: Internacional  
Descripción: 2024 L Latin American Computer Conference (CLEI)  
Ciudad: Buenos Aires, Argentina  
Año del evento: 2024  
Anales/Proceedings: 2024 L Latin American Computer Conference (CLEI)  
Publicación arbitrada  
Editorial: IEEE  
Palabras clave: Cyber range process mining training assessment  
Areas de conocimiento:  
Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información / Ingeniería de Sistemas y Comunicaciones / Cyber Ranges

DOI: [10.1109/clei64178.2024.10700452](https://doi.org/10.1109/clei64178.2024.10700452)  
<http://dx.doi.org/10.1109/clei64178.2024.10700452>  
Scopus

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

GUILLERMO GUERRERO , GUSTAVO BETARTE , JUAN DIEGO CAMPO

Publicado

Completo

Evento: Regional

Descripción: 2024 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

Editorial: IEEE

Palabras clave: Cyber range academic

Areas de conocimiento:

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

Ingeniería de Sistemas y Comunicaciones / Cyber Range

DOI: [10.1109/argencon62399.2024.10735713](https://doi.org/10.1109/argencon62399.2024.10735713)

<http://dx.doi.org/10.1109/argencon62399.2024.10735713>

**Consent validation for personal data access control using ABAC (2024)**

MARIA MOLINA , GUSTAVO BETARTE , CARLOS LUNA

Publicado

Resumen expandido

Evento: Regional

Descripción: LADC 2024: 13th Latin-American Symposium on Dependable and Secure Computing

Ciudad: Recife Brazil

Año del evento: 2024

Anales/Proceedings:Proceedings of the 13th Latin-American Symposium on Dependable and

Secure Computing

Publicación arbitrada

Editorial: ACM

Ciudad: New York, NY, USA

Palabras clave: consent validation access control ABAC

Areas 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

DOI: [10.1145/3697090.3699803](https://doi.org/10.1145/3697090.3699803)

Financiación/Cooperación:

Comisión Sectorial de Investigación Científica / Apoyo financiero, Uruguay

<https://doi.org/10.1145/3697090.3699803>

**Capturing the security expert knowledge in feature selection for web application attack detection (2024)**

AMANDA RIVEROL , GUSTAVO BETARTE , RODRIGO MARTÍNEZ , ALVARO PARDO

Publicado

Completo

Evento: Regional

Descripción: LADC 2024: 13th Latin-American Symposium on Dependable and Secure Computing

Ciudad: Recife Brazil

Año del evento: 2024

Anales/Proceedings:Proceedings of the 13th Latin-American Symposium on Dependable and

Secure Computing

Publicación arbitrada

Editorial: ACM

Ciudad: New York, NY, USA

Palabras clave: expert knowledge feature selection web application attack detection

Areas de conocimiento:

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

Computación / Lógica de la Programación, Métodos Formales, Seguridad Informática

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

Ingeniería de Sistemas y Comunicaciones / Seguridad Informática  
Medio de divulgación: Internet  
DOI: [10.1145/3697090.3699797](https://doi.org/10.1145/3697090.3699797)  
Financiación/Cooperación:  
Comisión Sectorial de Investigación Científica / Apoyo financiero, Uruguay  
<https://doi.org/10.1145/3697090.3699797>

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

G. BETARTE , JUAN DIEGO CAMPO , N. Serrano  
Publicado  
Completo  
Evento: Internacional  
Descripción: LADC '23: 12th Latin-American Symposium on Dependable and Secure Computing  
Ciudad: La Paz  
Año del evento: 2023  
Anales/Proceedings:LADC '23: Proceedings of the 12th Latin-American Symposium on Dependable and Secure Computing  
Publicación arbitrada  
Palabras clave: Trackers Mobile applications Privacy leaks  
Medio de divulgación: Internet  
DOI: <https://doi.org/10.1145/3615366.3615426>

**Discovering attacker profiles using process mining and the MITRE ATT&CK taxonomy (2023)**

G. BETARTE , D. calegari , M. Rodríguez  
Publicado  
Completo  
Evento: Internacional  
Descripción: LADC '23: 12th Latin-American Symposium on Dependable and Secure Computing  
Ciudad: La paz  
Año del evento: 2023  
Anales/Proceedings:LADC '23: Proceedings of the 12th Latin-American Symposium on Dependable and Secure Computing  
Publicación arbitrada  
Palabras clave: Attacker profilesprocess mining  
Medio de divulgación: Internet  
DOI: <https://doi.org/10.1145/3615366.3615372>

**A Security Analysis of a Referential Architecture of the FIWARE Platform (2023)**

G. BETARTE , J. PERATA  
Publicado  
Completo  
Evento: Internacional  
Descripción: 2023 XLIX Latin American Computer Conference (CLEI)  
Ciudad: La Paz  
Año del evento: 2023  
Anales/Proceedings:Proceedings of the 2023 XLIX Latin American Computer Conference (CLEI)  
Publicación arbitrada  
Palabras clave: FIWARE security assessment threat analysis  
Medio de divulgación: Internet  
DOI: [10.1109/CLEI60451.2023.10346164](https://doi.org/10.1109/CLEI60451.2023.10346164)

**An Idealized Model for the Formal Security Analysis of the Miblewimble Cryptocurrency Protocol (2022)**

G. BETARTE , LUNA, C. , A. SILVEIRA  
Publicado  
Completo  
Evento: Internacional  
Descripción: 2022 XLVIII Latin American Computer Conference (CLEI)  
Ciudad: Armenia, Colombia  
Año del evento: 2022  
Publicación arbitrada  
Palabras clave: Miblewimble Formal analysis Security  
DOI: [10.1109/CLEI56649.2022.9959925](https://doi.org/10.1109/CLEI56649.2022.9959925)

### **Web Application Attacks Detection Using Deep Learning (2021)**

NICOLÁS MONTES , GUSTAVO BETARTE , RODRIGO MARTÍNEZ , ALVARO PARDO

Publicado

Completo

Descripción: CIARP 2021

Año del evento: 2021

Anales/Proceedings: Progress in Pattern Recognition, Image Analysis, Computer Vision, and Applications

Volumen: 12702

Serie: LNCS

ISSN/ISBN: 9783030934194

Publicación arbitrada

Editorial: Springer International Publishing

Ciudad: Cham

Palabras clave: Web application firewall Anomaly detection Deep learning

Medio de divulgación: Internet

DOI: [10.1007/978-3-030-93420-0\\_22](https://doi.org/10.1007/978-3-030-93420-0_22)

[http://dx.doi.org/10.1007/978-3-030-93420-0\\_22](http://dx.doi.org/10.1007/978-3-030-93420-0_22)

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

GUSTAVO BETARTE , JUAN DIEGO CAMPO , ANDREA DELGADO , PABLO EZZATTI , LAURA GONZALEZ , ALVARO MARTIN , RODRIGO MARTINEZ , BARBARA MURACCIOLE

Publicado

Completo

Descripción: 2021 XLVII Latin American Computing Conference (CLEI)

Ciudad: Cartago, Costa Rica

Año del evento: 2021

Anales/Proceedings: 2021 XLVII Latin American Computing Conference (CLEI)

Publicación arbitrada

Editorial: IEEE

Palabras clave: COVID-19 proximity tracing protocols security privacy

DOI: [10.1109/clei53233.2021.9640202](https://doi.org/10.1109/clei53233.2021.9640202)

<http://dx.doi.org/10.1109/clei53233.2021.9640202>

### **Exploring the Application of Process Mining Techniques to Improve Web Application Security (2021)**

MARCELO BRUNO , PABLO IBANEZ , TAMARA TECHERA , DANIEL CALEGARI , GUSTAVO BETARTE

Publicado

Completo

Descripción: 2021 XLVII Latin American Computing Conference (CLEI)

Ciudad: Cartago, Costa Rica

Año del evento: 2021

Anales/Proceedings: 2021 XLVII Latin American Computing Conference (CLEI)

Publicación arbitrada

Editorial: IEEE

Palabras clave: Security web applications process mining web application firewall ModSecurity ProM

DOI: [10.1109/clei53233.2021.9640192](https://doi.org/10.1109/clei53233.2021.9640192)

<http://dx.doi.org/10.1109/clei53233.2021.9640192>

### **Design principles for constructing GDPR-compliant blockchain solutions (2021)**

FERNANDA MOLINA , GUSTAVO BETARTE , CARLOS LUNA

Publicado

Completo

Descripción: 2021 IEEE/ACM 4th International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB)

Ciudad: Madrid, Spain

Año del evento: 2021

Anales/Proceedings: 2021 IEEE/ACM 4th International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB)

Publicación arbitrada

Editorial: IEEE

Palabras clave: Blockchain Off-chain GDPR design principles security and privacy

Medio de divulgación: Internet

**Privacy-aware blockchain solutions: design and threat analysis (2021)**

G. BETARTE , C. LUNA , F. MOLINA

Publicado

Completo

Descripción: 24th Iberoamerican Conference on Software Engineering, ClbSE 2021

Ciudad: San Jose, Costa Rica

Año del evento: 2021

Anales/Proceedings:24th Iberoamerican Conference on Software Engineering

ISSN/ISBN: 978-1-7138-3944-6

Publicación arbitrada

Editorial: Curran Associates 2021

Palabras clave: Privacy-aware blockchain threat analysis

Medio de divulgación: Internet

**Towards a Formally Verified Implementation of the MimbleWimble Cryptocurrency Protocol (2020)**

G. BETARTE , M. CRISTIA , LUNA, C. , A. SILVEIRA , D. ZANARINI

Publicado

Completo

Evento: Internacional

Descripción: Applied Cryptography and Network Security Workshops. ACNS 2020

Año del evento: 2020

Anales/Proceedings:Zhou J. et al. (eds) Applied Cryptography and Network Security Workshops.

ACNS 2020

Volumen:1

Serie: Lecture Notes in Computer Science

Página inicial: 3

Página final: 23

ISSN/ISBN: 978-3-030-61638-0

Publicación arbitrada

Editorial: Springer

Palabras clave: Cryptocurrency protocols MimbleWimble Formal Verification

Áreas de conocimiento:

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

Computación / Formal Methods, Computer Security

Medio de divulgación: Internet

DOI: [https://doi.org/10.1007/978-3-030-61638-0\\_1](https://doi.org/10.1007/978-3-030-61638-0_1)

**Web application attacks detection using machine learning techniques (2018)**

G. BETARTE , ALVARO PARDO , R. MARTÍNEZ

Publicado

Completo

Evento: Internacional

Descripción: In 17th IEEE International Conference on Machine Learning and Applications,

Ciudad: Orlando

Año del evento: 2018

Anales/Proceedings:Proceedings of the 17th IEEE International Conference on Machine Learning and Applications, 2018.

Publicación arbitrada

Palabras clave: Application security WAF Machine Learning

Áreas de conocimiento:

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

Ingeniería de Sistemas y Comunicaciones / Seguridad Informática, Aprendizaje Automático

Medio de divulgación: Internet

Financiación/Cooperación:

Agencia Nacional de Investigación e Innovación / Apoyo financiero, Uruguay

**Improving Web Application Firewalls through Anomaly Detection (2018)**

G. BETARTE , ALVARO PARDO , E. Giménez , R. MARTÍNEZ

Publicado

Completo

Evento: Internacional

Descripción: Special Session on Big Data and Information Security of 17th IEEE International Conference on Machine Learning and Applications  
Ciudad: Orlando  
Año del evento: 2018  
Anales/Proceedings: Special Session on Big Proceedings of 17th IEEE International Conference on Machine Learning and Applications  
Publicación arbitrada  
Palabras clave: Application Security WAF Machine Learning Anomaly Detection  
Areas de conocimiento:  
Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información / Ingeniería de Sistemas y Comunicaciones / Seguridad Informática, Aprendizaje Automático  
Medio de divulgación: Internet  
Financiación/Cooperación:  
Agencia Nacional de Investigación e Innovación / Apoyo financiero, Uruguay

#### **Offloading Cryptographic Services to the SIM Card (2018)**

G. BETARTE , JAVIER BALIOSIAN , D. Pedraja  
Publicado  
Completo  
Evento: Internacional  
Descripción: 2018 Eighth Latin-American Symposium on Dependable Computing (LADC)  
Ciudad: Foz de Iguacu  
Año del evento: 2018  
Anales/Proceedings: Proceedings of the 2018 Eighth Latin-American Symposium on Dependable Computing (LADC)  
Publicación arbitrada  
Palabras clave: Smart Card Cryptography Offloading  
Areas de conocimiento:  
Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información / Ingeniería de Sistemas y Comunicaciones / Seguridad Informática, Gestión de redes  
Medio de divulgación: Internet  
Financiación/Cooperación:  
Agencia Nacional de Investigación e Innovación / Apoyo financiero, Uruguay

#### **Security in iOS and Android: A Comparative Analysis (2018)**

G. BETARTE , LUNA, C. , R. GALUPPO  
Publicado  
Completo  
Evento: Internacional  
Descripción: 2018 37th International Conference of the Chilean Computer Science Society (SCCC)  
Año del evento: 2018  
Anales/Proceedings: Proceedings of the 2018 37th International Conference of the Chilean Computer Science Society (SCCC)  
ISSN/ISBN: 1522-4902  
Publicación arbitrada  
Palabras clave: Seguridad Informática Android iOS  
Areas 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  
DOI: [10.1109/SCCC.2018.8705237](https://doi.org/10.1109/SCCC.2018.8705237)  
<https://ieeexplore.ieee.org/document/8705237>

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

G. BETARTE , J.D. CAMPO , F. GOROSTIAGA , C. LUNA  
Publicado  
Completo  
Evento: Internacional  
Descripción: The 27th International Symposium on Logic-Based Program Synthesis and Transformation (LOPSTR)  
Ciudad: Namur, Belgium  
Año del evento: 2017  
Anales/Proceedings: Informal Proceedings

Publicación arbitrada

Palabras clave: Reference monitor Permission model

Areas de conocimiento:

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

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Formal Methods, Security

Medio de divulgación: Internet

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

G. BETARTE , J. CAMPO , M. CRISTIÁ , F. GOROSTIAGA , C. LUNA , C. SANZ

Publicado

Completo

Evento: Internacional

Descripción: Simposio Latinoamericano de Ingeniería de Software - CLEI 2017

Ciudad: Córdoba, Argentina

Año del evento: 2017

Publicación arbitrada

Palabras clave: Android Model-based testing Security mechanisms

Areas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Formal Methods, Security

Medio de divulgación: Internet

#### **Privacy by Design: de la abstracción jurídica a la práctica ingenieril (2017)**

F. BALADÁN , G. BETARTE , A. BLANCO , C. MONTAÑA , B. MURACCIOLE , B. RODRÍGUEZ

Publicado

Completo

Evento: Internacional

Descripción: IX Congreso Iberoamericano de Seguridad Informática

Ciudad: Buenos Aires, Argentina

Año del evento: 2017

Publicación arbitrada

Palabras clave: Privacy by Design Desafío jurídico e ingenieros

Areas de conocimiento:

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

Medio de divulgación: Internet

#### **Towards model-driven virtual patching for web applications (2016)**

G. BETARTE , R. DE LA FUENTE , R. MARTÍNEZ , J. PIREZ , F. ZIPITRÍA

Publicado

Completo

Evento: Internacional

Descripción: Latin American Symposium on Dependable Computing

Ciudad: Cali

Año del evento: 2016

Publicación arbitrada

Palabras clave: Model-driven Virtual patching Web applications

Areas de conocimiento:

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

Medio de divulgación: Internet

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

G. BETARTE , C. LUNA , J.D. CAMPO , A. ROMANO

Publicado

Completo

Evento: Internacional

Descripción: 12th International Colloquium on Theoretical Aspects of Computing

Ciudad: Cali

Año del evento: 2015

Anales/Proceedings: Proceedings of ICTAC 2015: the 12th International Colloquium on Theoretical Aspects of Computing

Publicación arbitrada  
Palabras clave: Android Security Formal Methods  
Areas de conocimiento:  
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Seguridad Informática, Métodos Formales  
Medio de divulgación: Internet

**Machine-assisted Cyber Threat Analysis using Conceptual Knowledge Discovery (2015)**

G. BETARTE , M. BARRERE , ET AL  
Publicado  
Completo  
Evento: Internacional  
Descripción: 4th Workshop 'What can FCA do for Artificial Intelligence?'  
Ciudad: Buenos Aires  
Año del evento: 2015  
Anales/Proceedings: Proceedings of FCA4AI 2015: the 4th Workshop 'What can FCA do for Artificial Intelligence?'  
Publicación arbitrada  
Palabras clave: Knowledge discovery Cyber threat intelligence  
Areas de conocimiento:  
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Seguridad Informática, Knowledge Discovery  
Medio de divulgación: Internet

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

G. BETARTE , G. BARTHE , J.D. CAMPO , C. LUNA , D. PICHARDIE  
Publicado  
Completo  
Evento: Internacional  
Descripción: CCS'14 2014: the 21st ACM SIGSAC Conference on Computer and Communications Security  
Ciudad: Scottsdale, Arizona, USA  
Año del evento: 2014  
Anales/Proceedings: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security  
Pagina inicial: 1267  
Pagina final: 1279  
ISSN/ISBN: 978-1-4503-295  
Publicación arbitrada  
Editorial: ACM Press  
Ciudad: New York  
Palabras clave: Formal model and proofs Security  
Areas de conocimiento:  
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Seguridad, Métodos Formales  
Medio de divulgación: Internet  
DOI: [10.1145/2660267.2660283](https://doi.org/10.1145/2660267.2660283)  
[dl.acm.org/citation.cfm?id=2660267](https://dl.acm.org/citation.cfm?id=2660267)

**Formally verified implementation of an idealized model of virtualization (2013)**

G. BETARTE , G. BARTHE , J.D. CAMPO , C. LUNA  
Publicado  
Completo  
Evento: Internacional  
Descripción: 19th International Conference on Types for Proofs and Programs (TYPES 2013)  
Año del evento: 2013  
Volumen: 27  
Fascículo: 1  
Serie: LIPIcs  
Publicación arbitrada  
Palabras clave: Isolation Virtualization Formal model and proofs  
Areas de conocimiento:  
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Métodos formales, Seguridad

Medio de divulgación: Internet  
<http://www.dagstuhl.de/en/publications/lipics>

**Design and implementation of a Computer Security Diploma (2013)**

G. BETARTE , M. E. CORTI

Publicado

Completo

Evento: Internacional

Descripción: Conferencia Latinoamericana de Informática

Ciudad: Naiguana, Venezuela

Año del evento: 2013

Anales/Proceedings: Anales del CLEI 2013

Publicación arbitrada

Palabras clave: Security Diploma

Áreas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Seguridad

Medio de divulgación: Internet

<http://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?punumber=6661499>

**Cache-leakage Resilience Isolation in an Idealized Model of Virtualization (2012)**

G. BARTHE , G. BETARTE , J.D. CAMPO , C. LUNA

Publicado

Completo

Evento: Internacional

Descripción: 25th IEEE Computer Security Foundations Symposium (CSF 2012)

Ciudad: Cambridge, MA, USA

Año del evento: 2012

Anales/Proceedings: 25th IEEE Computer Security Foundations Symposium

Publicación arbitrada

Editorial: IEEE Computer Society Press

Palabras clave: Isolation Leakage resilience

Áreas de conocimiento:

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

Medio de divulgación: Internet

**Towards machine-assisted formal procedures for collection of digital evidence (2011)**

M. BARRERE , G. BETARTE , M. RODRÍGUEZ

Publicado

Completo

Evento: Internacional

Descripción: IX International Conference on Privacy, Security and Trust

Ciudad: Montreal, Quebec, Canada

Año del evento: 2011

Anales/Proceedings: Proceedings of PST 2011

ISSN/ISBN: 9781457705823

Publicación arbitrada

Editorial: IEEE Computer Society Press

Palabras clave: Digital forensics, automation, collection

Áreas de conocimiento:

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

Medio de divulgación: Internet

<http://dx.doi.org/10.1109/PST.2011.5971960>

**Un Framework para la Definición e Implantación de Mecanismos de Control de Acceso Basado en Roles, Contenidos e Información Contextual (2011)**

G. BETARTE

Publicado

Completo

Evento: Internacional

Descripción: VI Congreso Iberoamericano de Seguridad Informática

Ciudad: Bucaramanga, Colombia

Año del evento: 2011  
Anales/Proceedings: Anales del VI Congreso Iberoamericano de Seguridad Informática  
Pagina inicial: 32  
Pagina final: 35  
Publicación arbitrada  
Palabras clave: Seguridad aplicaciones, RBAC  
Areas de conocimiento:  
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Seguridad  
Medio de divulgación: Internet

**Formally verifying isolation and availability in an idealized model of virtualization (2011)**

G. BARTHE , G. BETARTE , J.D. CAMPO , C. LUNA  
Publicado  
Completo  
Evento: Internacional  
Descripción: FM 2011: the 17th International Symposium on Formal Methods  
Ciudad: Limerick, Ireland  
Año del evento: 2011  
Anales/Proceedings: Proceedings of FM 2011  
Volumen: 6664  
Pagina inicial: 231  
Pagina final: 245  
ISSN/ISBN: 0302-9743  
Publicación arbitrada  
Editorial: Springer  
Ciudad: Berlin  
Palabras clave: Virtualization Formal model Non-interference  
Areas de conocimiento:  
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Formal Methods, Security  
Medio de divulgación: Internet  
DOI: [10.1007/978-3-642-21437-0](https://doi.org/10.1007/978-3-642-21437-0)  
<http://www.springerlink.com/content/978-3-642-21436-3/#section=911240&page=1&locus=17>

**A Certified Access Controller for JME-MIDP 2.0 enabled Mobile Devices (2009)**

R. ROUSHANI , G. BETARTE , C. LUNA  
Publicado  
Completo  
Evento: Internacional  
Descripción: First Chilean Workshop on Formal Methods  
Ciudad: Punta Arenas, Chile  
Año del evento: 2009  
Anales/Proceedings: Proceedings of the Chilean Computer Science Society International Conference 2008  
Pagina inicial: 51  
Pagina final: 58  
ISSN/ISBN: 4244-7752-4  
Publicación arbitrada  
Editorial: IEEE-CS Press  
Palabras clave: Access Control, JME, Formal Methods  
Areas de conocimiento:  
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Métodos Formales, Seguridad Informática  
Medio de divulgación: Internet  
<http://dx.doi.org/10.1109/SCCC.2009.10>

**Formal Specification and Analysis of the MIDP 3.0 Security Model (2009)**

G. MAZEIKIS , G. BETARTE , C. LUNA  
Publicado  
Completo  
Evento: Internacional  
Descripción: First Chilean Workshop on Formal Methods  
Ciudad: Punta Arenas, Chile

Año del evento: 2009  
Anales/Proceedings: Proceedings of the Chilean Computer Science Society International Conference 2009  
Pagina inicial: 59  
Pagina final: 66  
ISSN/ISBN: 4244-7752-4  
Publicación arbitrada  
Editorial: IEEE CS Press  
Palabras clave: JME, Formal Methods  
Areas de conocimiento:  
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Métodos Formales, Seguridad Informática  
Medio de divulgación: Internet  
<http://dx.doi.org/10.1109/SCCC.2009.18>

**A Framework for the Analysis of Access Control Models for Interactive Mobile Devices (2009)**

G. BETARTE , J. M. CRESPO , C. LUNA  
Publicado  
Completo  
Evento: Internacional  
Descripción: Types for Proofs and Programs 2008  
Ciudad: Torino, Italy  
Año del evento: 2009  
Anales/Proceedings: Proceedings of the International Conference Types 2008  
Serie: LNCS  
Pagina inicial: 49  
Pagina final: 63  
ISSN/ISBN: 0302-9743  
Publicación arbitrada  
Editorial: Springer Berlin Heidelberg  
Ciudad: Berlin  
Palabras clave: Formal model Control access Mobile devices  
Areas de conocimiento:  
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Formal Methods, Security  
Medio de divulgación: Internet  
DOI: [10.1007/978-3-642-02444-3](https://doi.org/10.1007/978-3-642-02444-3)  
<http://www.springerlink.com/content/2511654x57211m8x/>

**Concepción, Diseño e Implantación de un Laboratorio de Seguridad Informática. (2007)**

M. E. CORTI , M. RODRÍGUEZ , G. BETARTE  
Publicado  
Completo  
Evento: Internacional  
Descripción: Congreso Iberoamericano de Seguridad Informática - CIBSI  
Ciudad: Mar del Plata, Argentina  
Año del evento: 2007  
Anales/Proceedings: Anales del Congreso Iberoamericano de Seguridad Informática  
Volumen: 1  
Publicación arbitrada  
Palabras clave: Laboratorio de Seguridad, Virtualización  
Areas de conocimiento:  
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Seguridad Informática  
Medio de divulgación: Otros

**A Formal Specification of the MIDP 2.0 Security Model. (2007)**

G. BETARTE , S. ZANELLA , C. LUNA  
Publicado  
Completo  
Evento: Internacional  
Descripción: Formal Aspects in Security and Trust 2006  
Ciudad: Ontario, Canada  
Año del evento: 2007

Anales/Proceedings:Fourth International Workshop, FAST 2006, Revised Selected Papers  
Volumen:4691  
Serie: LNCS  
Pagina inicial: 220  
Pagina final: 234  
ISSN/ISBN: 0302-9743  
Publicación arbitrada  
Editorial: Springer Berlin Heidelberg  
Ciudad: Berlin  
Palabras clave: Formal model Control access MIDP  
Areas de conocimiento:  
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Formal Methods, Security  
Medio de divulgación: Internet  
DOI: [10.1007/978-3-540-75227-1](https://doi.org/10.1007/978-3-540-75227-1)  
<http://www.springerlink.com/content/f518771177qg1514/>

#### **Hacia una Implementación Exitosa de un SGSI (2005)**

M. E. CORTI , G. BETARTE , R. DE LA FUENTE  
Publicado  
Completo  
Evento: Internacional  
Descripción: Congreso Iberoamericano de Seguridad Informática - CIBSI  
Ciudad: Valparaíso, Chile  
Año del evento: 2005  
Anales/Proceedings:Anales del Congreso Iberoamericano de Seguridad Informática  
Volumen:1  
Publicación arbitrada  
Palabras clave: SGSI, Metodología  
Areas de conocimiento:  
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Seguridad Informática  
Medio de divulgación: Otros

#### **FORMAVIE: Formal Modelling and Verification of the Java Card 2.1.1 Security Architecture. (2002)**

G. BETARTE , E. GIMÉNEZ , B. CHETALI , C. LOISEAUX  
Publicado  
Completo  
Evento: Internacional  
Descripción: eSmart Conference  
Ciudad: Niza  
Año del evento: 2002  
Anales/Proceedings:Proceedings of eSmart 2002  
Volumen:1  
Publicación arbitrada  
Palabras clave: Máquina Virtual, Java Card, Seguridad  
Areas de conocimiento:  
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Semántica Formal, Java  
Medio de divulgación: CD-Rom

#### **Specification of a Smart Card Operating System (2000)**

G. BETARTE , C. CORNES , N. SZASZ , A. TASISTRO  
Publicado  
Completo  
Evento: Internacional  
Descripción: Types for Proofs and Programs 1999  
Ciudad: Lökeberg, Sweden  
Año del evento: 2000  
Anales/Proceedings:Proceedings of the International Workshop, TYPES'99, Selected papers  
Volumen:1956  
Serie: LNCS  
Pagina inicial: 77  
Pagina final: 93

ISSN/ISBN: 0302-9743

Publicación arbitrada

Editorial: Springer Berlin Heidelberg

Ciudad: Berlin

Palabras clave: Formal model Smart Cards Operating System

Areas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Formal Methods, Security

Medio de divulgación: Internet

DOI: [10.1007/3-540-44557-9](https://doi.org/10.1007/3-540-44557-9)

<http://www.springerlink.com/content/wnfjvtxyh80mp403/>

#### **Dependent record types, subtyping and proof reutilization (1997)**

G. BETARTE

Publicado

Completo

Evento: Internacional

Descripción: Workshop on Subtyping, Inheritance and Modular Development of Proofs,

Ciudad: Durham, UK

Año del evento: 1997

Anales/Proceedings: Online Proceedings of the Workshop on Subtyping, Inheritance and Modular Development of Proofs,

Publicación arbitrada

Palabras clave: Type Theory, Dependent Records, Subtyping

Areas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Type Theory

Medio de divulgación: Internet

#### **Type Theory and Functional Programming: A work proposal (1996)**

G. BETARTE, ET AL

Publicado

Completo

Evento: Internacional

Descripción: 1st. Workshop on Functional Programming

Ciudad: Buenos Aires, Argentina

Año del evento: 1996

Anales/Proceedings: Proceedings, 1st. Workshop on Functional Programming

Publicación arbitrada

Palabras clave: Type Theory, Functional Programming

Areas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Type Theory

Medio de divulgación: Otros

#### **Formalisation of systems of algebras using dependent record types and subtyping: an example (1995)**

G. BETARTE

Publicado

Completo

Evento: Internacional

Descripción: Nordic Workshop of Programming

Ciudad: Göteborg, Suecia

Año del evento: 1995

Anales/Proceedings: Proceedings of the 7th. Nordic Workshop of Programming

Publicación arbitrada

Palabras clave: Type Theory, Dependent Records, Subtyping

Areas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Type Theory

Medio de divulgación: Otros

## PRODUCTOS

### **FORMAVIE: Formal Modelling and Verification of the Java Card 2.1.1 Security Architecture. (2002)**

Proyecto, Otra

G. BETARTE

Desarrollo de la especificación formal y prueba de propiedades de seguridad del proceso de verificación estática, carga y ejecución de aplicaciones applets en una tarjeta inteligente Java Card

País: Francia

Disponibilidad: Restringida

Producto con aplicación productiva o social: Apoyo para la implementación sin fallas de plataformas Java Card

Institución financiadora: Ministère des Finances - Projet OPPIDUM

Palabras clave: Formal Model, Java Card

Áreas de conocimiento:

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

Medio de divulgación: Otros

### **FOb: un intérprete para un lenguaje Orientado a Objetos basado en objetos. (2000)**

, Software

G. BETARTE

FOb es un intérprete para un lenguaje orientado a objetos basado en objetos y funcional.

País: Uruguay

Disponibilidad: Irrestringida

Palabras clave: Theory of Objects, Functional programming

Áreas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Theory of Objects

Medio de divulgación: Internet

<http://www.fing.edu.uy/inco/grupos/mf/Proyectos/Investigacion/TTSUBOBJ/Software/FOb/fob.tar.gz>

### **SubRec (1999)**

, Software

G. BETARTE

Subrec is a proof checker for an extension of Martin-Löf's theory of types with dependent record types and subtyping.

País: Uruguay

Disponibilidad: Irrestringida

Palabras clave: Type theory, dependent record types, subtyping

Áreas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Type Theory, Logical frameworks

Medio de divulgación: Internet

<http://www.fing.edu.uy/~gustun/SUBREC/>

## PROCESOS

### **Procédé pour le contrôle paramétrable de la sécurité de systèmes informatiques et systèmes embarqués mettant en œuvre ledit procédé. (2004)** Trabajo relevante

Proceso Productivo

G. BETARTE

Procedimientos para la definición e implementación de sistemas de controles de seguridad en sistemas informáticos, aplicables particularmente pero no exclusivamente a sistemas embebidos de limitados recursos de memoria y computación

País: Francia

Disponibilidad: Restringida

Proceso con aplicación productiva o social: Procedimientos de control de acceso para sistemas informáticos embebidos

Institución financiadora: Trusted Logic SA, Versailles, France.

Patente o Registro:

Patente de invención

FR2864657 (A1), Contrôle paramétrable de la sécurité

Depósito: 23/10/2003; Examen: ; Concesión: 13/09/2004

Patente nacional: NO

Palabras clave: Control de acceso, Sistemas embebidos

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://fr.espacenet.com/publicationDetails/biblio?](http://fr.espacenet.com/publicationDetails/biblio?KC=A1&date=20050701&NR=2864657A1&DB=fr.espacenet.c)

[KC=A1&date=20050701&NR=2864657A1&DB=fr.espacenet.c](http://fr.espacenet.com/publicationDetails/biblio?KC=A1&date=20050701&NR=2864657A1&DB=fr.espacenet.c)

Patente francesa nro. FR2864657 (A1), aprobada por el Institut National de la Propriété

Industrielle (INPI) de Francia. El inventor, Gustavo Betarte, ha cedido esta patente a la empresa francesa Trusted Logic SA como parte de su contrato laboral con la misma.

## TRABAJOS TÉCNICOS

### Informe PENCTI - Área TIC (2008)

Consultoría

G. BETARTE

Consultoría de Análisis, Diagnóstico y Prospección del área de TICs cuyo resultado servirá como insumo en la confección del Plan Estratégico Nacional para la Ciencia, Tecnología e Innovación

País: Uruguay

Idioma: Español

Ciudad: Montevideo

Disponibilidad: Irrestringida

Número de páginas: 47

Duración: 6 meses

Institución financiadora: BID

Palabras clave: TIC

Áreas de conocimiento:

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

Medio de divulgación: Internet

<http://www.anii.org.uy/imagenes/ConsultoriaTICs.pdf>

### Java Card System Protection Profile Collection (2003)

Consultoría

G. BETARTE

The Java Card Protection Profile provides a modular set of security requirements designed specifically for the characteristics of the Java Card platform.

País: Francia

Idioma: Inglés

Ciudad: Versalles, Francia

Disponibilidad: Irrestringida

Número de páginas: 195

Duración: 12 meses

Institución financiadora: Sun Microsystems Inc.

Palabras clave: Protection Profile, Java Card

Áreas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Seguridad Informática

Medio de divulgación: Internet

<http://java.sun.com/javacard/pp.html>

## Evaluaciones

### EVALUACIÓN DE PROYECTOS

#### COMITÉ EVALUACIÓN DE PROYECTOS

#### ANII - Programa STIC Amsud (2014 / 2019)

/ , Uruguay

Cantidad: Mas de 20

ANII - Programa STIC Amsud

Participa en calidad de representante de la ANII en el Comité Científico del programa de colaboración franco - sudamericano STIC Amsud.

## **EVALUACIÓN INDEPENDIENTE DE PROYECTOS**

### **Programa Paraguayo para el Desarrollo de la Ciencia y Tecnología – PROCIENCIA ( 2016 )**

Paraguay

CONACYT

Cantidad: Menos de 5

### **Proyectos de Investigación Científica y Tecnológica ( 2015 / 2020 )**

Argentina

Fondo Nacional de Ciencia y Tecnología

Cantidad: Menos de 5

### **ANII - Programa STIC Amsud ( 2014 / 2019 )**

Uruguay

ANII - Programa STIC Amsud

Cantidad: Mas de 20

Participa en calidad de representante de la ANII en el Comité Científico del programa de colaboración franco - sudamericano STIC Amsud.

### **Fondo Nacional de Ciencia y Tecnología ( 2008 / 2020 )**

Argentina

Fondo Nacional de Ciencia y Tecnología

Cantidad: De 5 a 20

### **Latin American and Caribbean Collaborative ICT Research Federation (LACCIR) ( 2007 / 2010 )**

Uruguay

Latin American and Caribbean Collaborative ICT Research Federation (LACCIR)

Cantidad: Menos de 5

Latin American and Caribbean Collaborative ICT Research Federation is an international network of Latin American and Caribbean Universities connected by their Information and Communication Technologies and Computer Science Departments, sponsored by Microsoft Research, Inter American Development Bank, Organization of American States, and Local Government Agencies.

## **EVALUACIÓN DE PUBLICACIONES**

### **COMITÉ EDITORIAL**

#### **IEEE Transactions on Cloud Computing ( 2013 / 2013 )**

Cantidad: Menos de 5

#### **Special Issue of the Journal of Functional Programming: Dependent Type Theory meets Practical Programming (JFP, Cambridge University Press) ( 2002 / 2002 )**

Cantidad: Menos de 5

### **REVISIONES**

#### **Annals of Operations Research ( 2019 )**

Tipo de publicación: Anales

Cantidad: Menos de 5

#### **Journal of Network and Computer Applications ( 2019 / 2024 )**

Tipo de publicación: Revista

Cantidad: De 5 a 20

#### **New Generation Computing ( 2018 )**

Tipo de publicación: Revista

Cantidad: Menos de 5

**IEEE Transactions on Information Forensics and Security ( 2018 )**

Tipo de publicación: Revista

Cantidad: Menos de 5

**The Computer Journal ( 2017 )**

Tipo de publicación: Revista

Cantidad: Menos de 5

**EVALUACIÓN DE EVENTOS Y CONGRESOS**

**Formal Methods Europe ( 2018 / 2020 )**

Comité programa congreso

Arbitrado

**Latin-American Symposium on Dependable Computing - Student Forum ( 2018 )**

Comité programa congreso

Brasil

Arbitrado

**FormaliSE 2017 : FME Workshop on Formal Methods in Software Engineering ( 2017 )**

Comité programa congreso

Argentina

Arbitrado

IEEE, ACM

**10th International Workshop on Security and Trust Management ( 2016 )**

Comité programa congreso

Grecia

Arbitrado

ERCIM

**12th International Colloquium on Theoretical Aspects of Computing ( 2015 )**

Comité programa congreso

Colombia

Arbitrado

CLEI, Microsoft Research

**10th International Conference on Availability, Reliability and Security ( 2015 )**

Revisiones

Francia

TWU, SBA Research

**10th International Symposium on Formal Aspects of Component Software ( 2013 )**

Revisiones

China

**Latina American Formal Methods Workshop ( 2013 )**

Comité programa congreso

Argentina

Arbitrado

**Certified Programas and Proofs 2013 ( 2013 )**

Revisiones  
Australia

**9th International Conference on Software Engineering and Formal methods ( 2011 )**

Comité programa congreso  
Uruguay  
Arbitrado

**Workshop de Seguridad Informática - JAIIO ( 2010 / 2014 )**

Comité programa congreso  
Argentina  
Arbitrado

SADIO

**Conference of the Chilean Computer Science Society ( 2007 / 2020 )**

Revisiones  
Chile

**European Symposium on research in Computer Security (ESORICS) ( 2006 / 2008 )**

Revisiones

**Congreso Iberoamericano de Seguridad Informática ( 2005 / 2020 )**

Comité programa congreso  
España  
Arbitrado

**International Conference on Logic for Programming, Artificial Intelligence and Reasoning ( 2004 / 2008 )**

Revisiones

**FME 2003: International Symposium on Formal Methods Europe ( 2003 )**

Revisiones  
Italia

**International Summer School in Semantics and Applications ( 2003 )**

Uruguay

Promotor, miembro del comité científico y co-organizador de la International Summer School in Semantics and Applications que fue desarrollada en Montevideo, en julio de 2003. Esta escuela fue organizada por investigadores del INRIA Sophia-Antipolis, doctores Gilles Barthe y Davide Sangiorgi, y por un equipo de investigadores del InCo, cuyo responsable fue quien suscribe. La

escuela nucleó numerosos investigadores de renombre internacional, que dictaron cursos sobre temas fundacionales y avanzados de Teoría de la Programación, Semántica de Lenguajes y Seguridad, constituyendo, aparte de ser la primer escuela de este tipo organizada en América Latina, un evento científico relevante para la Ciencia de la Computación en el Cono Sur. Los lecturers de la escuela fueron los siguientes investigadores: Dr. Gilles Barthe, INRIA Sophia-Antipolis, Francia Dr. Peter Dybjer, Chalmers University of Technology, Suecia Dr. Marcelo Fiore, Cambridge University, UK Dr. Joshua Guttman, The Mitre Corporation, USA Dr. Andrei Sabelfeld, Chalmers University of Technology, Suecia Dr. Davide Sangiorgi, INRIA Sophia-Antipolis, Francia Dr. David Schmidt, University of Kansas, USA Dr. Colin Stirling, University of Edinburgh, UK La escuela contó con el respaldo y soporte económico del organismo internacional CIMPA (Centre International de Mathématiques Pures et Appliquées) y del ICTP (International Centre for Theoretical Physics).

#### **Conferencia Latinoamericana de Estudios en Informática ( 2000 / 2020 )**

Comité programa congreso  
Arbitrado

CLEI

#### **Mathematics of Program Construction ( 2000 / 2004 )**

Revisiones

#### **Workshop on Types for Proofs and Programs ( 1997 / 2006 )**

Revisiones

#### **Symposium on Principles of Programming Languages ( 1996 / 2001 )**

Revisiones

ACM SIGACT - SIGPLAN

### **EVALUACIÓN DE PREMIOS**

#### **Premio a Tesis de Doctorado del Pedeciba Informática ( 2017 / 2024 )**

Evaluación de premios y concursos  
Uruguay

Cantidad: Menos de 5  
Pedeciba Informática

#### **Premio a Tesis de Maestría del Pedeciba Informática ( 2017 / 2020 )**

Evaluación de premios y concursos  
Uruguay

Cantidad: Menos de 5  
Área Informática del Pedeciba

#### **Premio ANIU a Proyectos de grado ( 2016 / 2017 )**

Evaluación de premios y concursos  
Uruguay

Cantidad: Menos de 5  
Academia Nacional de Ingeniería - Uruguay

#### **Premio ANIU a Tesis de Posgrado ( 2011 / 2019 )**

Evaluación de premios y concursos  
Uruguay

Cantidad: De 5 a 20  
Academia Nacional de Ingeniería - Uruguay

### **Premio Joven Investigador del Pedeciba - Área Informática ( 2011 )**

Evaluación de premios y concursos  
Uruguay

Cantidad: Menos de 5  
Pedeciba

### **Miembro del Jurado del Concurso Latinoamericano de Tesis de Maestría en Informática ( 1998 / 2012 )**

Uruguay

Cantidad: De 5 a 20  
CLEI-UNESCO

## **EVALUACIÓN DE CONVOCATORIAS CONCURSABLES**

### **Miembro del Jurado del Concurso Latinoamericano de Tesis de Maestría en Informática ( 1998 / 1999 )**

Uruguay

Cantidad: Menos de 5  
CLEI (Centro Latinoamericano de Estudios en Informática) - UNESCO

### **Integrante de comisiones asesoras y tribunales en concursos para proveer cargos de Profesor Agregado (Gr. 4), Profesor Adjunto (Gr. 3) y Asistente (Gr. 2) ( 1998 / 2009 )**

Uruguay

Cantidad: De 5 a 20  
Instituto de Computación de la Facultad de Ingeniería, UDELAR

## **JURADO DE TESIS**

### **Magister en Ingeniería Eléctrica ( 2019 )**

Jurado de mesa de evaluación de tesis  
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería / Instituto de Ingeniería Eléctrica , Uruguay  
Nivel de formación: Maestría

### **PhD in Computer Science ( 2017 )**

Jurado de mesa de evaluación de tesis  
Sector Extranjero/Internacional/Otros / Kungliga Tekniska Högskolan , Suecia

### **Doctor en Informática ( 2011 / 2024 )**

Jurado de mesa de evaluación de tesis  
Sector Educación Superior/Público / Programa de Desarrollo de las Ciencias Básicas / Área Informática (PEDECIBA) / Instituto de Computación, Facultad de Ingeniería, UdelAR, Uruguay  
Nivel de formación: Doctorado

### **Magister en Informática ( 1997 / 2024 )**

Jurado de mesa de evaluación de tesis  
Sector Educación Superior/Público / Programa de Desarrollo de las Ciencias Básicas / Área Informática (PEDECIBA) / Instituto de Computación, Facultad de Ingeniería, UdelAR, Uruguay  
Nivel de formación: Maestría

## **Formación de RRHH**

### **TUTORÍAS CONCLUIDAS**

### **POSGRADO**

### **Process mining-based Assessment of Cyber Range Trainings (2022 - 2025)**

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 en pie de igualdad ( G. BETARTE , JUAN DIEGO CAMPO )  
Nombre del orientado: Guillermo Guerrero  
País: Uruguay  
Palabras Clave: Process mining Cyber range Training assessment  
Areas de conocimiento:  
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Lógica de la Programación, Métodos Formales, Seguridad Informática

**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 / Universidad de la República / Facultad de Ingeniería / Instituto de Computación , Uruguay  
Programa: Maestría en Informática (PEDECIBA - UdelaR)  
Tipo de orientación: Cotutor en pie de igualdad ( G. BETARTE , JUAN DIEGO CAMPO )  
Nombre del orientado: Nicolás Serrano  
País: Uruguay  
Palabras Clave: COVID-19 Privacy leaks Trackers

**A formal analysis of the Mumblewimble cryptocurrency protocol with a security approach (2020 - 2022)**

Tesis de maestría  
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería / Instituto de Computación , Uruguay  
Programa: Maestría en Informática (PEDECIBA - UdelaR)  
Tipo de orientación: Cotutor en pie de igualdad ( G. BETARTE , LUNA, C. )  
Nombre del orientado: Adrián Silveira  
País: Uruguay  
Palabras Clave: Cryptocurrency protocol Security MumbleWimble  
Areas de conocimiento:  
Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información / Ingeniería de Sistemas y Comunicaciones / Métodos Formales, Seguridad Informática

**Análisis de Seguridad de la plataforma de ciudades inteligentes Fiware (2020 - 2022)**

Tesis de maestría  
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería / Instituto de Computación , Uruguay  
Programa: Maestría en Computación  
Tipo de orientación: Tutor único o principal  
Nombre del orientado: Juan Pablo Perata  
País: Uruguay  
Palabras Clave: Fiware Análisis de seguridad Ciudades inteligentes  
Areas de conocimiento:  
Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información / Ingeniería de Sistemas y Comunicaciones / Seguridad Informática

**Constructing privacy aware blockchain solutions: Design guidelines and threat analysis techniques (2018 - 2021)**

Tesis de maestría  
Sector Educación Superior/Público / Programa de Desarrollo de las Ciencias Básicas / Área Informática (PEDECIBA) / Instituto de Computación , Uruguay  
Programa: Maestría en Informática  
Tipo de orientación: Cotutor en pie de igualdad ( G. BETARTE , LUNA, C. )  
Nombre del orientado: Fernanda Molina  
País: Uruguay  
Palabras Clave: Blockchain Procesos Off-chain  
Areas de conocimiento:  
Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información / Ingeniería de Sistemas y Comunicaciones / Blockchain

**Neural networks for Application Security (2018 - 2021)**

Tesis de maestría  
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería / Instituto de Computación , Uruguay  
Programa: Maestría en Ingeniería (Ingeniería Matemática)  
Tipo de orientación: Cotutor en pie de igualdad ( G. BETARTE , ALVARO PARDO )  
Nombre del orientado: Nicolás Montes  
País: Uruguay  
Palabras Clave: Neural networks Probabilistic Models Application Security  
Areas de conocimiento:  
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación e Información / Computer Security, Anomaly Detection

#### **Identification and Classification of Web Application Attacks using Machine Learning Techniques**

Tesis de maestría  
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería , Uruguay  
Tipo de orientación: Cotutor en pie de igualdad  
Nombre del orientado: Rodrigo Martínez  
País: Uruguay  
Palabras Clave: Security Web Application Firewall Machine Learning  
Areas de conocimiento:  
Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información / Ingeniería de Sistemas y Comunicaciones / Seguridad Informática

#### **Offloading cryptographic services to the SIM card in smartphones**

Tesis de maestría  
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería , Uruguay  
Tipo de orientación: Tutor único o principal  
Nombre del orientado: Daniel Pedraja  
País: Uruguay  
Palabras Clave: Secure Offloading Dispositivos móviles  
Areas de conocimiento:  
Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información / Ingeniería de Sistemas y Comunicaciones / Seguridad

#### **Formally Verified Countermeasures Against Cache Based Attacks in Virtualization Platforms**

Tesis de doctorado  
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería , Uruguay  
Programa: Doctorado en Informática (UDELAR-PEDECIBA)  
Tipo de orientación: Cotutor en pie de igualdad  
Nombre del orientado: Juan Diego Campo  
País: Uruguay  
Palabras Clave: Seguridad Informática, Métodos Formales  
Areas de conocimiento:  
Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información / Ingeniería de Sistemas y Comunicaciones / Seguridad Informática, Métodos Formales

#### **Formal analysis of security models for mobile devices, virtualization platforms, and domain name systems**

Tesis de doctorado  
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería , Uruguay  
Programa: Doctorado en Informática (UDELAR-PEDECIBA)  
Nombre del orientado: Carlos Luna  
País: Uruguay  
Palabras Clave: Formal model and proofs Security  
Areas de conocimiento:  
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Seguridad, Métodos Formales

#### **Metodología de Implantación y Seguimiento de SGSI en ISPs**

Tesis de maestría  
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería , Uruguay  
Programa: Maestría en Ingeniería en Computación  
Nombre del orientado: Gustavo Pallas

País: Uruguay  
Palabras Clave: SGSI, Metodología  
Areas de conocimiento:  
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Seguridad Informática

#### **Model-Driven Approach to the Development of Correct Information-Intensive Software Components**

Tesis de maestría  
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería , Uruguay  
Programa: Maestría en Informática (UDELAR-PEDECIBA)  
Nombre del orientado: Daniel Perovich  
País: Uruguay  
Palabras Clave: MDD, Formal methods  
Areas de conocimiento:  
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Object Oriented Systems, Model Driven Development

#### **Towards Secure Distributed Computations**

Tesis de maestría  
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería , Uruguay  
Programa: Maestría en Informática (UDELAR-PEDECIBA)  
Nombre del orientado: Felipe Zipitría  
País: Uruguay  
Palabras Clave: Proof Carrying Results  
Areas de conocimiento:  
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Seguridad Informática, Métodos Formales

#### **Análisis y Automatización de la Implantación de SGSI en Empresas Uruguayas**

Tesis de maestría  
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería , Uruguay  
Programa: Maestría en Ingeniería en Computación  
Nombre del orientado: María Eugenia Corti  
País: Uruguay  
Palabras Clave: SGSI, Metodología  
Areas de conocimiento:  
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Gestión de la Seguridad de la Información

#### **The Reflex Sandbox : an experimentation environment for an aspect-oriented Kernel**

Tesis de maestría  
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería , Uruguay  
Programa: Maestría en Informática (UDELAR-PEDECIBA)  
Nombre del orientado: Leonardo Rodríguez  
País: Uruguay  
Palabras Clave: Aspect Oriented Programming  
Areas de conocimiento:  
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Object Oriented Systems, Aspect Oriented Programming

#### **A Formal Semantics of State Modification Primitives of Object-oriented Systems**

Tesis de maestría  
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería , Uruguay  
Programa: Maestría en Informática (UDELAR-PEDECIBA)  
Nombre del orientado: Andrés Vignaga  
País: Uruguay  
Palabras Clave: Object Oriented Systems, Primitives, Formal  
Areas de conocimiento:  
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Object Oriented Systems, Formal Methods

**GRADO**

### **CyRa.uy: Hacia un cyber range académico (2022 - 2023)**

Tesis/Monografía de grado  
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería / Instituto de Computación , Uruguay  
Programa: Ingeniero en Computación  
Tipo de orientación: Cotutor en pie de igualdad ( G. BETARTE , JUAN DIEGO CAMPO )  
Nombre del orientado: Gabriel Corujo, Manuel Rodríguez  
País: Uruguay  
Palabras Clave: Cyber range Académico  
Areas de conocimiento:  
Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información / Ingeniería de Sistemas y Comunicaciones / Seguridad Informática

### **Reingeniería del Laboratorio de Seguridad Informática (2021 - 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 ( G. BETARTE , R. MARTÍNEZ , M. RODRÍGUEZ )  
Nombre del orientado: Rodrigo Gallardo, Guillermo Guerrero  
País: Uruguay  
Palabras Clave: Cyber ranges Laboratorio Seguridad Informática

### **WACE: Un integrador de clasificadores de ataques web (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 ( G. BETARTE , R. MARTÍNEZ , M. RODRÍGUEZ )  
Nombre del orientado: Fernando Outeda, Ezequiel Cuttica  
País: Uruguay  
Palabras Clave: ModSecurity Decision Engine

### **Web Honeypot**

Tesis/Monografía de grado  
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería / Instituto de Computación , Uruguay  
Tipo de orientación: Tutor único o principal  
Nombre del orientado: Federico Pernas, Agustín Sánchez, Nicolás Zeballos  
País: Uruguay  
Palabras Clave: Honeypot Aplicaciones Web  
Areas de conocimiento:  
Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información / Ingeniería de Sistemas y Comunicaciones / Seguridad Informática

### **Análisis de seguridad del protocolo DLMS/COSEM en el contexto de Smart Grids**

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 Márquez, Gabriel Rodríguez  
País: Uruguay  
Palabras Clave: Smart Grid DLMS/COSEM Smart Meter AMI IoT  
Areas de conocimiento:  
Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información / Ingeniería de Sistemas y Comunicaciones / Smart Grid, IoT, Seguridad Informática

### **Contramedidas para la manipulación maliciosa de dispositivos en LoRaWAN**

Tesis/Monografía de grado  
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería / Instituto de Computación , Uruguay  
Tipo de orientación: Tutor único o principal  
Nombre del orientado: Sebastian Passaro, Martín Pacheco

País: Uruguay

Palabras Clave: Seguridad Informática LoRaWAN LoRa IoT modelado de amenazas

Áreas de conocimiento:

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

#### **Minería de procesos para la mejora de la seguridad de aplicaciones web**

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: Tamara Techera, Pablo Ibáñez y Marcelo Bruno

País: Uruguay

Palabras Clave: Minería de procesos Seguridad Informática WAF Modsecurity Prom

Áreas de conocimiento:

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

#### **WAFIntl Security Inspector**

Tesis/Monografía de grado

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

Tipo de orientación: Tutor único o principal

Nombre del orientado: Leonardo Alberro

País: Uruguay

Palabras Clave: ModSecurity Eventos Seguridad Informática

Áreas de conocimiento:

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

#### **Detección de Anomalías para el Aseguramiento de Aplicaciones Web**

Tesis/Monografía de grado

Sector Educación Superior/Público / Universidad de la República / Facultad de Ciencias Económicas y de Administración / Instituto de Estadística, Uruguay

Tipo de orientación: Cotutor en pie de igualdad

Nombre del orientado: Nicolás Montes

País: Uruguay

Palabras Clave: Seguridad de Aplicaciones Web Detección de anomalías Modelos probabilísticos

Áreas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Modelos probabilísticos, Detección de anomalías

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Modelos Probabilísticos, Detección de Anomalías

#### **Mecanismos de soporte de Privacy by Design en Bases de Datos**

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: Guillermo Rodríguez

País: Uruguay

Palabras Clave: Privacy by Design Bases de datos

Áreas de conocimiento:

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

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

#### **Especificación e implementación de un prototipo certificado del sistema de permisos de Android**

Tesis/Monografía de grado

Sector Extranjero/Internacional/Otros / Universidad Nacional de Rosario, Argentina

Programa: Licenciatura en Ciencia de la Computación

Tipo de orientación: Cotutor en pie de igualdad

Nombre del orientado: Felipe Gorostiaga  
País: Argentina  
Palabras Clave: Verificación formal Android Modelo de permisos  
Áreas de conocimiento:  
Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información / Ingeniería de Sistemas y Comunicaciones / Seguridad  
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Métodos Formales, Seguridad Informática

#### **Especificación formal del modelo de 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  
Palabras Clave: Verificación formal Android Modelo de permisos  
Áreas de conocimiento:  
Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información / Ingeniería de Sistemas y Comunicaciones / Seguridad  
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Métodos Formales, Seguridad Informática

#### **DEPSA: Framework para la Definición y Enforcement de Políticas de Seguridad sobre Aplicaciones Web.**

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: Rodrigo de la Fuente, Luis González, Juan Pirez  
País: Uruguay  
Palabras Clave: Aplicaciones web Políticas de seguridad Automatización  
Áreas de conocimiento:  
Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información / Ingeniería de Sistemas y Comunicaciones / Seguridad

#### **Hacia la especificación y verificación formal de algoritmos criptográficos: Mini-AES certificado**

Tesis/Monografía de grado  
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería , Uruguay  
Programa: Ingeniería en Computación  
Tipo de orientación: Tutor único o principal  
Nombre del orientado: Mauricio Martínez, Enrique Rodríguez  
País: Uruguay  
Palabras Clave: Coq Criptografía certificada  
Áreas de conocimiento:  
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Métodos formales, Seguridad

#### **Descripción y análisis del modelo de seguridad de Android**

Tesis/Monografía de grado  
Sector Extranjero/Internacional/Otros / Facultad de Ciencias Económicas y Estadística de la Universidad Nacional de Rosario , Argentina  
Programa: Licenciatura en Ciencias de la Computación  
Nombre del orientado: Agustín Romano  
País: Argentina  
Palabras Clave: Android Modelo de seguridad Coq  
Áreas de conocimiento:  
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Métodos formales, Seguridad

#### **Análisis de evidencia digital obtenida de dispositivos móviles**

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

Programa: Ingeniería en Computación  
Nombre del orientado: Germán González, Horacio Pérez  
País: Uruguay  
Palabras Clave: Android Análisis de evidencia digital  
Areas de conocimiento:  
Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información / Ingeniería de Sistemas y Comunicaciones / Análisis Forense Digital

#### **Recolección de evidencia digital sobre dispositivos móviles**

Tesis/Monografía de grado  
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería , Uruguay  
Programa: Ingeniería en Computación  
Nombre del orientado: Juan Andrés Diana, José Ignacio Varela  
País: Uruguay  
Palabras Clave: recolección evidencia digital Android  
Areas de conocimiento:  
Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información / Ingeniería de Sistemas y Comunicaciones / Análisis Forense Digital

#### **Advanced threats: information sharing and collaboration**

Tesis/Monografía de grado  
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería , Uruguay  
Programa: Ingeniería en Computación  
Nombre del orientado: Julio Saráchaga  
País: Uruguay  
Palabras Clave: APTs information sharing collaboration  
Areas de conocimiento:  
Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información / Ingeniería de Sistemas y Comunicaciones / Análisis Forense Digital

#### **Sharing Theat Indicators**

Tesis/Monografía de grado  
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería , Uruguay  
Programa: Ingeniería en Computación  
Nombre del orientado: Eduardo Lapaz, Anthony Méndez  
País: Uruguay  
Palabras Clave: Threat Indicators Correlation  
Areas de conocimiento:  
Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información / Ingeniería de Sistemas y Comunicaciones / Análisis Forense Digital

#### **Análisis de Modelos de Memoria en Plataformas de Virtualización. Formalización de un prototipo de plataforma con Cache y TLB**

Tesis/Monografía de grado  
Sector Extranjero/Internacional/Otros / Facultad de Ciencias Exactas, Ingeniería y Agrimensura - UNR , Argentina  
Programa: Licenciatura en Ciencia de la Computación  
Nombre del orientado: Mauricio Chimento  
País: Argentina  
Palabras Clave: Memorias cache  
Areas de conocimiento:  
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Seguridad, Métodos Formales

#### **Especificación y Verificación formal de un modelo idealizado 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: Julio Pérez  
País: Uruguay  
Palabras Clave: virtualization, formal verification, security  
Areas de conocimiento:  
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la

**Prueba formal de algoritmos de firma digital y sus implementaciones usando asistentes de pruebas**

Tesis/Monografía de grado  
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería , Uruguay  
Programa: Ingeniería en Computación  
Nombre del orientado: Adrián Silveira  
País: Uruguay  
Palabras Clave: Criptografía, verificación formal  
Areas de conocimiento:  
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Criptografía y Métodos Formales

**Análisis de Modelos y Lenguajes de Autorización Descentralizada**

Tesis/Monografía de grado  
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería , Uruguay  
Programa: Ingeniería en Computación  
Nombre del orientado: Claudia Guinovart, Alejandro Berardinelli  
País: Uruguay  
Palabras Clave: Controls de acceso, lenguajes, políticas  
Areas de conocimiento:  
Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información / Ingeniería de Sistemas y Comunicaciones / Seguridad, Lenguajes

**Análisis de Malware**

Tesis/Monografía de grado  
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería , Uruguay  
Programa: Ingeniería en Computación  
Nombre del orientado: Ignacio Esmite, Nicolás Farías  
País: Uruguay  
Palabras Clave: Malware, Seguridad Informática  
Areas de conocimiento:  
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Seguridad Informática

**Design and Development of a framework for IT security training**

Tesis/Monografía de grado  
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería , Uruguay  
Programa: Ingeniería en Computación  
Nombre del orientado: Juan Diego Campo, Lucía Escanella, Carlos Pintado  
País: Uruguay  
Palabras Clave: IT Security Training  
Areas de conocimiento:  
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Seguridad Informática

**Automatización de Procesos en Análisis Forense Informático**

Tesis/Monografía de grado  
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería , Uruguay  
Programa: Ingeniería en Computación  
Nombre del orientado: Martín Barrere  
País: Uruguay  
Palabras Clave: Análisis Forense Digital Recolección de evidencia digital  
Areas de conocimiento:  
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Seguridad Informática

**Aplicación de Técnicas de Análisis de Código, para asegurar aplicaciones Web**

Tesis/Monografía de grado  
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería , Uruguay  
Programa: Ingeniería en Computación  
Nombre del orientado: Mario del Riego  
País: Uruguay

Palabras Clave: Seguridad de Aplicaciones Web

Áreas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Seguridad Informática

#### **Un Framework para el Análisis de Modelos de Control de Acceso para Dispositivos Móviles Interactivos**

Tesis/Monografía de grado

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

Programa: Licenciatura en Ciencia de la Computación

Nombre del orientado: Juan Manuel Crespo

País: Argentina

Palabras Clave: Seguridad, dispositivos móviles

Áreas de conocimiento:

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

#### **Un Controlador de Accesos Certificado para Dispositivos Móviles con JME-MIDP 2.0**

Tesis/Monografía de grado

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

Programa: Licenciatura en Ciencia de la Computación

Nombre del orientado: Ramin Roushani

País: Argentina

Palabras Clave: Seguridad, dispositivos móviles

Áreas de conocimiento:

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

#### **Especificación Formal del Modelo RBAC en el Cálculo de Construcciones Inductivas**

Tesis/Monografía de grado

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

Programa: Licenciatura en Ciencia de la Computación

Nombre del orientado: Cristian Rosa

País: Argentina

Palabras Clave: Control de acceso, modelo formal

Áreas de conocimiento:

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

#### **Modelo de datos para una Honeynet**

Tesis/Monografía de grado

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

Programa: Ingeniería en Computación

Nombre del orientado: Osvaldo Barrios, Mauricio Farías

País: Uruguay

Palabras Clave: Honeynets

Áreas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Seguridad Informática

#### **Automatización de actividades de implantación y mejora continua de un SGSI**

Tesis/Monografía de grado

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

Programa: Ingeniería en Computación

Nombre del orientado: Matías Gelós, Nicolás de Matto

País: Uruguay

Palabras Clave: SGSI, Metodología, Automatización

Áreas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Seguridad Informática

### **Diseño e implantación de un Honeypot**

Tesis/Monografía de grado  
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería , Uruguay  
Programa: Ingeniería en Computación  
Nombre del orientado: Fernando Cocco, Mauricio Garcia, María José Roullier  
País: Uruguay  
Palabras Clave: Honeypots, Honeynets  
Areas de conocimiento:  
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Seguridad Informática

### **Arcasa: Un framework para la definición y aplicación de políticas de control de acceso en sistemas de aplicación**

Tesis/Monografía de grado  
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería , Uruguay  
Programa: Ingeniería en Computación  
Nombre del orientado: Andrés Gatto, Rodrigo Martínez  
País: Uruguay  
Palabras Clave: Control de acceso, Sistemas de aplicaciones  
Areas de conocimiento:  
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Seguridad Informática

### **Especificación Formal del Modelo de Seguridad de MIDP 2.0 en el Cálculo de Construcciones Inductivas**

Tesis/Monografía de grado  
Sector Extranjero/Internacional/Otros / Facultad de Ciencias Exactas, Ingeniería y Agrimensura - UNR , Argentina  
Programa: Licenciatura en Ciencia de la Computación  
Nombre del orientado: Santiago Zanella  
País: Argentina  
Palabras Clave: Seguridad, dispositivos móviles  
Areas de conocimiento:  
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Seguridad, Métodos Formales

### **Semántica Formal de un subconjunto de Java.**

Tesis/Monografía de grado  
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería , Uruguay  
Programa: Ingeniería en Computación  
Nombre del orientado: Mercedes Saez, Ramona Zerpa  
País: Uruguay  
Palabras Clave: Semántica Formal, Java  
Areas de conocimiento:  
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Semántica Formal, Java

### **Especificación Formal de la Máquina Virtual Java Card.**

Tesis/Monografía de grado  
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería , Uruguay  
Programa: Ingeniería en Computación  
Nombre del orientado: Leonardo Grandillo, Jorge Erlich  
País: Uruguay  
Palabras Clave: Máquina Virtual, Java Card  
Areas de conocimiento:  
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Sistemas Embebidos

### **Tecnología Java Card**

Tesis/Monografía de grado  
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería , Uruguay  
Programa: Ingeniería en Computación  
Nombre del orientado: Daniel Perovich, Leonardo Rodríguez, Martín Varela  
País: Uruguay

Palabras Clave: Java Card

Áreas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Sistemas Embebidos

## TUTORÍAS EN MARCHA

### POSGRADO

#### **Feature selection and automated learning for web application attack detection (2023)**

Tesis de doctorado

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

Programa: Doctorado en Informática

Tipo de orientación: Tutor único o principal

Nombre del orientado: Amanda Riverol

País/Idioma: Uruguay,

Palabras Clave: Feature selection Automated learning Attack detection

Áreas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Seguridad Informática, Aprendizaje automático

La candidatura fue aceptada en el programa de doctorado pero todavía no está inscrita formalmente ya que es extranjera y está en procesos de homologar los créditos obtenidos en su tesis de maestría realizada en Cuba.

#### **A Knowledge based Tool for Cyber Threat Intelligence (2015)**

Tesis de doctorado

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

Programa: Doctorado en Informática

Tipo de orientación: Tutor único o principal

Nombre del orientado: Marcelo Rodríguez

País/Idioma: Uruguay, Español

Palabras Clave: Knowledge discovery Cyber threat intelligence Process Mining

Áreas de conocimiento:

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

El estudiante está en fase final de su tesis.

### GRADO

#### **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: Ingeniero en Computación

Tipo de orientación: Asesor

Nombre del orientado: Agustín De Leon, Tobías Iroa

País/Idioma: Uruguay,

Palabras Clave: WACE Clasificadores Ataques Web

Áreas de conocimiento:

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

## Otros datos relevantes

### PREMIOS, HONORES Y TÍTULOS

#### **Miembro del subgrupo D2, Movilidad y Apps, asesor del Grupo Asesor Científico Honorario (GACH). (2020)**

(Nacional)

Universidad de la República

El Grupo Asesor Científico Honorario (GACH), conformado por el Dr. Rafael Radi, como

coordinador general, y los Dres. Fernando Paganini y Henry Cohen, asesoran científicamente a la Presidencia de la República desde el 16 de abril en el camino hacia ¿la nueva normalidad?. El GACH realiza recomendaciones científicas en las áreas de salud y ciencia de datos al equipo de gobierno Transición UY.

## PRESENTACIONES EN EVENTOS

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

Congreso

Este evento presentará una exposición de Gustavo Betarte moderada por Rafael Páez donde conversarán sobre la plataforma de Cyberrange de Ciberlac y se explorarán las capacidades de esta herramienta.

Bolivia

Tipo de participación: Conferencista invitado

Carga horaria: 2

Nombre de la institución promotora: Universidad Mayor Real y Pontificia de San Francisco Xavier de Chuquisaca

Alcance geográfico: Regional Palabras Clave: Plataforma de Cyberrange Ciberlac

Áreas de conocimiento:

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

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

Simposio

En el marco de las celebraciones de los 10 años del Laboratorio de Ciberseguridad del Centro de Investigación en Computación, el Instituto Politécnico Nacional extiende una cordial invitación a miembros de la comunidad académica y público interesado en asistir al Coloquio de Ciberseguridad CIC 2024, donde se abordará el estado actual y retos de la investigación, el desarrollo de la tecnología y la formación de especialistas para el desarrollo de la ciber-resiliencia Latinoamericana. El programa del Coloquio es integrado por especialistas nacionales e internacionales que compartirán su conocimiento en conferencias magistrales, paneles de discusión, escuela de otoño de criptografía, talleres prácticos y sesión de posters estudiantil.

México

Tipo de participación: Expositor oral

Carga horaria: 2

Nombre de la institución promotora: Laboratorio de Ciberseguridad, CIC, Instituto Politécnico Nacional

Alcance geográfico: Internacional Palabras Clave: Formación científicos y tecnólogos en ciberseguridad América Latina

Áreas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Lógica de la Programación, Métodos Formales, Seguridad Informática

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

### **Congreso internacional de Tecnología y Aplicaciones informáticas JIT CITA 2023 (2023)**

Congreso

Aplicación de técnicas de aprendizaje automático y minería de procesos en la construcción de herramientas de ciber-inteligencia En esta charla presentaremos los principales resultados del proyecto de investigación WAFMind. Este proyecto tiene como objetivos proponer mecanismos que permitan incrementar la seguridad de sistemas computacionales adaptando técnicas de aprendizaje automático y aprendizaje profundo y el modelado del comportamiento de atacantes humanos y automatizados utilizando técnicas de minería de procesos. Describiremos un enfoque que combina técnicas de clasificación basadas en aprendizaje automático y profundo con conocimiento codificado en un WAF (Web Application Firewall) ampliamente implementado para prevenir ataques a aplicaciones web. Vamos a presentar los avances y resultados obtenidos durante el desarrollo del proyecto

Paraguay

Tipo de participación: Conferencista invitado

Carga horaria: 2

Nombre de la institución promotora: Facultad de Ciencias y Tecnologías, Universidad Católica "Nuestra Señora de la Asunción"

Alcance geográfico: Regional Palabras Clave: Técnicas de aprendizaje automático y minería de procesos Herramientas de ciber-inteligencia

Áreas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Lógica de la Programación, Métodos Formales, Seguridad Informática  
Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información / Ingeniería de Sistemas y Comunicaciones / Seguridad Informática

#### **12th Latin-American Symposium on Dependable and Secure Computing (2023)**

Congreso

Keynote presenting the results of the WAFMind project: Enhancing cyber-threat intelligence with the support of automated learning and process mining techniques.

Bolivia

Tipo de participación: Conferencista invitado

Carga horaria: 2

Nombre de la institución promotora: Western Parana State University, Brazil and Udelar

Alcance geográfico: Internacional Palabras Clave: WAFMind Seguridad adaptativa Aprendizaje automático

Áreas de conocimiento:

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

#### **Conferencia Latinoamericana de Estudios en Informática (2023)**

Congreso

Charla magistral presentando resultados del proyecto de investigación WAFMind: Enhancing cyber-threat intelligence with the support of automated learning and process mining techniques

Bolivia

Tipo de participación: Conferencista invitado

Carga horaria: 2

Nombre de la institución promotora: CLEI

Alcance geográfico: Regional Palabras Clave: WAFMind Seguridad adaptativa Aprendizaje automático

Áreas de conocimiento:

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

#### **SegurInfo Uruguay - 2014 (2014)**

Congreso

Formación (extra) curricular en Seguridad Informática

Uruguay

Tipo de participación: Conferencista invitado

Carga horaria: 1

Nombre de la institución promotora: Segurinfo

#### **Encuentro CUTI - InCo 2014 (2014)**

Seminario

Actividades de I+D+i del grupo de Seguridad Informática

Uruguay

Tipo de participación: Expositor oral

Carga horaria: 1

Nombre de la institución promotora: CUTI e Instituto de Computación, Facultad de Ingeniería, Udelar Palabras Clave: Seguridad Informática

#### **Seminario del InCo (2014)**

Seminario

Dataflow problems, Kildall's algorithm and applications

Uruguay

Tipo de participación: Expositor oral

Carga horaria: 2

Nombre de la institución promotora: InCo Palabras Clave: Dataflow problem, Kildall algorithm, security

#### **Envuetro de Lógica y Métodos Formales (2014)**

Seminario

Formalized static analysis of constant-time cryptographic algorithms

Uruguay

Tipo de participación: Expositor oral

Carga horaria: 16

Nombre de la institución promotora: ORT Uruguay e InCo Palabras Clave: static analysis constant time crypto algorithms

Areas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Formal Methods, Security

#### **Jornadas de Ciencia de la Computación (2014)**

Encuentro

Formalized static analysis of constant-time cryptographic algorithms

Uruguay

Tipo de participación: Conferencista invitado

Carga horaria: 24

Nombre de la institución promotora: Departamento de Ciencia de la Computación, FCEIA, Rosario, Argentina Palabras Clave: Formal model static analysis constant time crypto algorithms

Areas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Formal Methods, Security

#### **Encuentro de Lógica y Métodos Formales (2013)**

Seminario

VirtualCert: A certified idealized model of virtualization

Uruguay

Tipo de participación: Expositor oral

Carga horaria: 16

Nombre de la institución promotora: ORT Uruguay e InCo Palabras Clave: Virtualization Formal model Non-interference

Areas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Formal Methods, Security

#### **34th International Conference on Data Protection (2012)**

Congreso

Herramientas Forenses: lo que nuestros dispositivos dicen de nosotros

Uruguay

Tipo de participación: Panelista

Carga horaria: 4

Nombre de la institución promotora: AGESIC Palabras Clave: Análisis Forense Digital

Areas de conocimiento:

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

#### **Software Engineering and Formal Methods 2011 (2011)**

Taller

Tutorial invitado "Formal specification and verification of an idealized model of virtualization"

Uruguay

Tipo de participación: Expositor oral

Carga horaria: 3

Nombre de la institución promotora: Instituto de Computación Palabras Clave: Métodos Formales y Seguridad

Areas de conocimiento:

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

#### **Taller de Gestión de Incidentes de Seguridad Informática del Proyecto Amparo (2010)**

Taller

Taller de Gestión de Incidentes de Seguridad Informática del Proyecto Amparo

Chile

Tipo de participación: Expositor oral

Nombre de la institución promotora: LACNIC Palabras Clave: Seguridad Informática

Areas de conocimiento:

**II Workshop de Seguridad Informática / JAIIO (2010)**

Congreso  
Formal Specification of Access Control Mechanisms for Interactive Mobile Devices  
Argentina  
Tipo de participación: Expositor oral  
Carga horaria: 1  
Nombre de la institución promotora: SADIO Palabras Clave: formal models, proof assistants  
Áreas de conocimiento:  
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Formal Methods, Security

**REVVIS: REUNIÃO DE ESPECIALISTAS EM VERIFICAÇÃO E VALIDAÇÃO DE SOFTWARE (2007)**

Encuentro  
Especificación y Verificación Formal de Sistemas Críticos en el Instituto de Computación de la Universidad de la República (Uruguay)  
Brasil  
Tipo de participación: Expositor oral  
Carga horaria: 24  
Nombre de la institución promotora: CESAR - UNFEP, Brasil

**Workshop Formal Methods in Security, Seminario Anual STIC-AMSUD (2007)**

Taller  
Formal Specification of the J2ME Architecture,  
Uruguay  
Tipo de participación: Expositor oral  
Carga horaria: 40  
Nombre de la institución promotora: Instituto de Computación, Facultad de Ingeniería, UDELAR  
Palabras Clave: Formal Methods, Embedded Systems  
Áreas de conocimiento:  
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Métodos Formales, Seguridad Informática

**Séminaire Annuel du Réseau National des Technologies Logicielles (2003)**

Encuentro  
Le Projet EVA (Explication et Vérification Automatique de protocoles cryptographiques)  
Francia  
Tipo de participación: Expositor oral  
Carga horaria: 16  
Nombre de la institución promotora: Laboratoire VERIMAG

**Research Seminars (2002)**

Seminario  
A Type Theory based setting for Security Evaluation of multi-application Smart Card Platforms  
Suecia  
Tipo de participación: Conferencista invitado  
Carga horaria: 2  
Nombre de la institución promotora: Dept. of Computing Science, Chalmers University of Technology, Gothenburg Palabras Clave: Formal Methods, Smart Cards, Security  
Áreas de conocimiento:  
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Métodos formales, Seguridad

**Research Seminar (2000)**

Seminario  
Specification and Correctness of a (Small) Smart Card Operating System,  
Francia  
Tipo de participación: Conferencista invitado  
Carga horaria: 2  
Nombre de la institución promotora: Grupo Oasis, INRIA Sophia-Antipolis

### **Workshop on Subtyping and Dependent Types (2000)**

Congreso  
Type checking Dependent (Record) Types and Subtyping.  
Portugal  
Tipo de participación: Expositor oral  
Carga horaria: 2  
Nombre de la institución promotora: Departamento de Informática, Universidad do Minho  
Palabras Clave: Record Types, Type checking  
Areas de conocimiento:  
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Métodos Formales, Type Theory

### **TYPES Workshop on Subtyping, inheritance and modular development of proofs (1997)**

Taller  
Dependent Record Types, Subtyping and Proof Reutilization  
Inglaterra  
Tipo de participación: Expositor oral  
Carga horaria: 32  
Nombre de la institución promotora: UNiversity of Durham

### **The 7th. Nordic Workshop on the Theory of Programming (1995)**

Taller  
Formalization of Systems of Algebras Using Dependent Record Types and Subtyping: An Example.  
Suecia  
Tipo de participación: Expositor oral  
Carga horaria: 36  
Nombre de la institución promotora: Dept. of Computing Science, Chalmers University of Technology, Gothenburg

### **Workshop on Constructive Mathematics in Type Theory (1993)**

Taller  
The Integers form an Integral Domain.  
Italia  
Tipo de participación: Expositor oral  
Carga horaria: 32  
Nombre de la institución promotora: Università de Torino

## **JURADO/INTEGRANTE DE COMISIONES EVALUADORAS DE TRABAJOS ACADÉMICOS**

### **Opportunistic Network Modelling and Algorithms (2024)**

Candidato: Jorge Visca  
Tipo Jurado: Tesis de Doctorado  
G. BETARTE , ÁLVARO MARTÍN  
Doctorado en Informática / Sector Educación Superior/Público / Programa de Desarrollo de las Ciencias Básicas / Área Informática (PEDECIBA) / Uruguay  
País: Uruguay  
Idioma: Inglés  
Palabras Clave: Opportunistic Networks Modelling

### **Statically Identifying Web Vulnerabilities using Deep Learning (2022)**

Candidato: Héloïse Maurel  
Tipo Jurado: Tesis de Doctorado  
G. BETARTE  
INFORMATIQUE / Sector Extranjero/Internacional/Otros / Institución Extranjera / Université Côte d'Azur / Francia  
País: Francia  
Idioma: Inglés  
Palabras Clave: Web Vulnerabilities Deep Learning Static identification

### **Resource Allocation and Management Techniques for Network Slicing in WiFi Networks (2019)**

Candidato: Matías Richart  
Tipo Jurado: Tesis de Doctorado  
G. BETARTE

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

País: Uruguay

Idioma: Inglés

Palabras Clave: Resource allocation Management WiFi networks

Areas de conocimiento:

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

#### **On the Formalisation of the Metatheory of the Lambda Calculus and Languages with Binders (2017)**

Candidato: Ernesto Copello

Tipo Jurado: Tesis de Doctorado

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

País: Uruguay

Idioma: Inglés

Palabras Clave: Lambda Calculus Formal Metatheory

Areas de conocimiento:

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

#### **Secure System Virtualization: End-to-End Verification of Memory Isolation (2017)**

Candidato: Hamed Nemati

Tipo Jurado: Tesis de Doctorado

Programa de Doctorado / Sector Extranjero/Internacional/Otros / Institución Extranjera / Royal Institut of Technology in Stockholm / Suecia

País: Suecia

Idioma: Inglés

Palabras Clave: Secure Virtualization Memory Isolation

Areas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Formal Methods, Security

#### **Reasoning about Functional Programs by Combining Interactive and Automatic Proofs (2014)**

Candidato: Andrés Sicard

Tipo Jurado: Tesis de Doctorado

N. SZASZ, DANIEL FRIDLENDER, A. MIQUEL, M. JASKELIOFF

Doctorado en Informática (UDELAR-PEDECIBA) / Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería / Uruguay

País: Uruguay

Idioma: Español

Palabras Clave: Certified Functional Programming

Areas de conocimiento:

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

#### **RON - Opportunistic Networking (2013)**

Candidato: Jorge Visca

Tipo Jurado: Tesis de Maestría

ZAMBENEDETTI, VIERA

Maestría en Informática (UDELAR-PEDECIBA) / Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería / Uruguay

País: Uruguay

Idioma: Inglés

Palabras Clave: Opportunistic networks

Areas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Networking

#### **Inferencia de Tipos de Sesión (2012)**

Candidato: Ernesto Copello

Tipo Jurado: Tesis de Maestría

FERNANDO PAGANINI, DANIEL FRIDLENDER

Maestría en Ingeniería / Sector Educación Superior/Privado / Universidad ORT Uruguay / Facultad de Ingeniería / Uruguay

País: Uruguay

Idioma: Español

Palabras Clave: Tipos de sesión Algoritmo de inferencia Verificación formal

Áreas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Cálculos de Procesos, Teoría de Tipos

#### **Models and algorithms for the optimal design of bus routes in public transportation systems (2011)**

Candidato: Antonio Mauttone

Tipo Jurado: Tesis de Doctorado

M. GENDREAU

Doctorado en Informática (UDELAR-PEDECIBA) / Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería / Uruguay

País: Uruguay

Idioma: Español

#### **AGENT-BASED METHODOLOGY FOR DEVELOPING AGROECOSYSTEMS' SIMULATIONS (2011)**

Candidato: Jorge Corral

Tipo Jurado: Tesis de Maestría

A. MAUTONNE , P. BOMMEL

Maestría en Ingeniería en Computación / Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería / Uruguay

País: Uruguay

Idioma: Inglés

#### **A Proposal Towards Low Human Interaction in Network Intrusion Detection Systems (Propuesta de tesis de Doctorado) (2011)**

Candidato: Carlos Catania

Tipo Jurado: Otras

Doctorado en Ciencias de la Computación / Sector Extranjero/Internacional/Otros / Institución Extranjera / Universidad Nacional del Centro de la Provincia de Buenos Aires / Argentina

País: Argentina

Idioma: Inglés

#### **HFusion: a fusion tool based on Acid Rain puls extensions (2009)**

Candidato: Facundo Domínguez

Tipo Jurado: Tesis de Maestría

Maestría en Informática (UDELAR-PEDECIBA) / Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería / Uruguay

País: Uruguay

Idioma: Inglés

Palabras Clave: Deforestation. Acid Rain

Áreas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Programación genérica

#### **Carga de un Data Warehouse a partir de la traza de diseño (2007)**

Candidato: Ignacio Larrañaga

Tipo Jurado: Tesis de Maestría

Maestría en Informática (UDELAR-PEDECIBA) / Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería / Uruguay

Sitio Web: <http://www.fing.edu.uy/inco/pedeciba/bibliote/tesis/tesism-larranaga.pdf>

País: Uruguay

Idioma: Español

Palabras Clave: Data Warehouse

Áreas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Sistemas de Información, Data Warehouses

#### **A machine-assisted Proof of the subject reduction property for a small typed functional language. (1995)**

Candidato: Ana Bove  
 Tipo Jurado: Tesis de Maestría  
 Maestría en Informática (UDELAR-PEDECIBA) / Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería / Uruguay  
 País: Uruguay  
 Idioma: Inglés  
 Palabras Clave: Subject reduction, functional languages  
 Areas de conocimiento:  
 Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Functional Languages, Logical Frameworks

## CONSTRUCCIÓN INSTITUCIONAL

Soy docente del Instituto de Computación de la Facultad de Ingeniería desde diciembre de 1986. Desde mayo de 2010 soy Profesor Titular efectivo de ese Instituto. En 2006 fundé, y dirijo desde ese año, el Grupo de Seguridad Informática del InCo, que es el único equipo que desarrolla investigación y docencia en esa disciplina en la Udelar.

Soy el responsable académico de la Especialización y de la Maestría en Seguridad Informática de Facultad de Ingeniería.

He sido en tres oportunidades Coordinador del Área Informática del Pedeciba y he sido miembro del Consejo Científico de esa área desde el año 2010 al 2020 y del año 2022 al 2024

Desde junio de 2022 a junio de 2024 fui el Presidente de la Red CiberLac, que es una red de excelencia en Ciberseguridad para América Latina y el Caribe. Esta red nuclea 26 Universidades e Institutos de investigación de la región. Actualmente soy el representante de Uruguay en el Comité Ejecutivo de la red.

## Información adicional

Representante de ANII en el Comité Científico del programa de colaboración franco-sudamericano STIC AMSUD (2012-2016).

## Indicadores de producción

<b>ACTIVIDADES</b>	<b>60</b>
<b>Líneas de investigación</b>	5
<b>Proyectos Investigación Desarrollo</b>	19
<b>Docencia</b>	16
<b>Extensión</b>	1
<b>Gestión Académica</b>	15
<b>Dirección Administración</b>	1
<b>Servicio Técnico Especializado</b>	3
<b>PRODUCCIÓN BIBLIOGRÁFICA</b>	<b>78</b>
<b>Artículos publicados en revistas científicas</b>	17
Completo	17
<b>Trabajos en eventos</b>	43
<b>Libros y Capítulos</b>	3
Libro publicado	2
Capítulos de libro publicado	1
<b>Documentos de trabajo</b>	15
Completo	15
<b>PRODUCCIÓN TÉCNICA</b>	<b>6</b>

<b>Productos tecnológicos</b>	3
<b>Procesos o técnicas</b>	1
Con registro o patente	1
<b>Trabajos técnicos</b>	2
<b>EVALUACIONES</b>	<b>40</b>
<b>Evaluación de proyectos</b>	6
<b>Evaluación de eventos</b>	21
<b>Evaluación de publicaciones</b>	7
<b>Evaluación de convocatorias concursables</b>	2
<b>Jurado de tesis</b>	4
<b>FORMACIÓN RRHH</b>	<b>57</b>
<b>Tutorías/Orientaciones/Supervisiones concluidas</b>	54
Tesis de maestría	14
Tesis/Monografía de grado	38
Tesis de doctorado	2
<b>Tutorías/Orientaciones/Supervisiones en marcha</b>	3
Tesis de doctorado	2
Tesis/Monografía de grado	1