

# VI CONGRESO IBEROAMERICANO DE SEGURIDAD INFORMÁTICA CIBSI 2011

Noviembre 2, 3 y 4  
Bucaramanga, Colombia



POLITÉCNICA



Universidad  
Pontificia  
Bolivariana  
SECCIONAL BUCARAMANGA



*Actas del VI Congreso Iberoamericano de Seguridad Informática  
CIBSI 2011*

Bucaramanga, Colombia, 2 al 4 de Noviembre de 2011

**Editores**

Angélica Flórez Abril  
Jorge Ramió Aguirre  
Arturo Ribagorda Garnacho  
Jeimy J. Cano Martínez

ISBN: 978-958-8506-18-0

©2011

Facultad de Ingeniería Informática, Universidad Pontificia Bolivariana, Seccional Bucaramanga,  
Colombia

Universidad Politécnica de Madrid, España

## Prefacio

El Congreso Iberoamericano de Seguridad Informática (CIBSI) es una iniciativa de la Red Temática de Criptografía y Seguridad de la Información. Desde el año 2002 se ha venido desarrollando, tomando en cuenta durante los primeros años la realización con frecuencia anual y a partir del año 2003 se realiza cada dos años.

La primera versión del CIBSI fue desarrollada en el año 2002 en Morelia, México; en el año 2003 se celebra la segunda edición en Ciudad de México; en el año 2005 se realizó la tercera edición en Valparaíso, Chile; la cuarta edición tiene lugar en el año 2007 en Mar del Plata, Argentina; y en el año 2009 se celebra la quinta versión en Montevideo, Uruguay.

Este año 2011, se desarrolla la sexta versión del congreso, teniendo como sede la Universidad Pontificia Bolivariana de Bucaramanga, Colombia, institución educativa que desde el año 2005 se encuentra ofreciendo programas de educación continua en seguridad de la información y a partir del año 2007 ofrece la Especialización en Seguridad Informática, convirtiéndose de ésta manera en una institución que apalanca el desarrollo docente e investigación en seguridad de la información en Colombia.

Para los investigadores del área de seguridad de la información en Colombia, es muy grato realizar por primera vez el CIBSI 2011, evento que facilita el intercambio de conocimiento y la formación de redes de colaboración en el ámbito de la investigación y el desarrollo en seguridad de la información.

Dentro de la agenda programada del evento se tienen definidos tres espacios: conferencias magistrales, ponencias de los trabajos presentados y el Primer Taller Iberoamericano de Enseñanza e Innovación Educativa en Seguridad de la Información (TIBETS).

Se realizarán tres conferencias magistrales por parte de reconocidos investigadores en el área, tales como el Dr. Sergio Rajsbaum de la Universidad Nacional Autónoma de México, el Dr. Justo Carracedo de la Universidad Politécnica de Madrid y el Dr. Jeimy Cano de la Universidad Pontificia Bolivariana de Bucaramanga.

Este documento contiene los trabajos a ser presentados como ponencias por investigadores de diversos países a nivel de Iberoamérica. Se recibieron 39 trabajos, de los cuales el Comité del Programa seleccionó 23 trabajos provenientes de los siguientes países: Argentina, Cuba, Colombia, España, Venezuela, Uruguay, México y Brasil.

Como nuevo aporte, en el marco del CIBSI se realizará el TIBETS, espacio que se dedicará a presentar las experiencias en enseñanza e innovación educativa en el área de seguridad de la información, nuevos rumbos docentes, análisis de proyectos de colaboración conjunta y programas de posgrados, que permita plantear estrategias de colaboración docente.

Se espera que estas actas y las reflexiones realizadas del 2 al 4 de noviembre en el Campus de la Universidad Pontificia Bolivariana de Bucaramanga sirvan para el fortalecimiento de la investigación en seguridad de la información, la generación de nuevos espacios de discusión y el estrechamiento de lazos interinstitucionales para el avance en programas de posgrados y rumbos docentes en el área.

## Organización de la Conferencia

### Comité Organizador General

Angélica Flórez Abril, Universidad Pontificia Bolivariana, Colombia  
Jorge Ramió Aguirre, Universidad Politécnica de Madrid, España

### Comité Organizador Logístico

Angélica Flórez Abril, Universidad Pontificia Bolivariana, Colombia  
Jeimy Cano Martínez, Universidad Pontificia Bolivariana, Colombia  
Reinaldo Mayol Arnao, Universidad Pontificia Bolivariana, Colombia

### Comité Técnico

Reinaldo Mayol Arnao, Universidad Pontificia Bolivariana, Colombia  
Con el apoyo de los estudiantes de Ingeniería Informática:  
Miguel Gerardo Mateus Marín y Julián Eduardo Ramírez Rico

### Comité del Programa

Jeimy Cano (Chair)	Universidad Pontificia Bolivariana
Arturo Ribagorda Garnacho (Chair)	Universidad Carlos III de Madrid
Marco Aurélio Amaral Henriques	State University of Campinas - Unicamp
Nicolás Antezana Abarca	Sociedad Peruana de Computación
Javier Areitio Bertolín	Universidad de Deusto
Gustavo Betarte	Universidad de la República
Joan Borrel Viader	Universidad Autónoma de Barcelona
Pino Caballero Gil	Universidad de La Laguna
Adriano Mauro Cansian	Universidad Estadual Paulista
Enrique Daltabuit Godas	Universidad Nacional Autónoma de México
Ángel Martín Delrey	Universidad de Salamanca
Josep Domingo-Ferrer	Universidad Rovira i Virgili
Josep Lluís Ferrer-Gomilla	Universidad de las Islas Baleares
Amparo Fúster-Sabater	Consejo Superior de Investigaciones Científicas
Juan Pedro Hecht	Universidad de Buenos Aires
Luis Hernandez Encinas	Consejo Superior de investigación
Emilio Hernández	Universidad Simón Bolívar
Leobardo Hernández Audelo	Universidad Nacional Autónoma de México
Julio César López	Universidad Estatal de Campinas
Vincenzo Mendillo	Universidad Central de Venezuela
Josep María Miret Biosca	Universidad de Lleida
Gaspar Modelo-Howard	Universidad Tecnológica de Panamá
Raul Monge	Universidad Técnica Federico Santa María
Guillermo Morales-Luna	Centro de Investigación y Estudios Avanzados

Alberto Peinado Domínguez

Josep Rifà Coma

Jorge Blasco Alis

Hugo Francisco González Robledo

José María de Fuentes García-Romero de  
Tejada

del IPN

Universidad de Malaga

Universidad Autónoma de Barcelona

Universidad Carlos III de Madrid

Universidad Politécnica de San Luis de Potosí

Universidad Carlos III de Madrid

## Tabla de contenido

Extended Visual Cryptography Scheme with an Artificial Cocktail Party Effect.....	1
<i>Agustín Moreno Cañadas and Nelly Paola Palma Vanegas</i>	
A Non-Reducible Meyer-Müller's Like Elliptic Curve Cryptosystem .....	11
<i>Santi Martínez, Josep M. Miret, Francesc Sebé and Rosana Tomás</i>	
SAFET: Sistema para la generación de aplicaciones con firma electrónica.....	15
<i>Victor Bravo Bravo and Antonio Araujo Brett</i>	
Computational Intelligence Applied on Cryptology: a brief review .....	23
<i>Moisés Danziger and Marco Aurélio Amaral Henrique</i>	
New Possibilities for using Cellular Automata in Cryptography .....	36
<i>Mauro Tardivo Filho and Marco A. A. Henriques</i>	
Métricas de seguridad en los SGSIs, para conocer el nivel de seguridad de los SSOO y de los SGBD .....	45
<i>Luis Enrique Sánchez Crespo, Antonio Santos-Olmo Parra, Eduardo Fernández-Medina and Mario Piattini</i>	
e-PULPO: Gestión de la Seguridad de la Información con Software Libre.....	53
<i>Ana Matas Martín and Andrés Mendez</i>	
Definición de un modelo automatizado para la evaluación y mantenimiento de un SGSI.....	64
<i>Daniel Villafranca, Eduardo Fernández-Medina and Mario Piattinia</i>	
La Gestión de Riesgos y Controles en Sistemas de Información.....	79
<i>Marlene Lucila Guerrero Julio and Lu´ Carlos Gómez Flórez</i>	
Esquema de Micropago Anónimo, Equitativo y no Rastreado: Aplicación a los Servicios LBS.....	85
<i>Andreu Pere Isern-Dey`, Llorenç, Huguet-Rotger, Magdalena Payeras-Capellá and Maciá Mut Puigserver</i>	
A Zero Knowledge Authentication Protocol using Non Commutative Groups .....	96
<i>Juan Pedro Hecht</i>	
Caracterización del entorno de riesgo de los niños, niñas y adolescentes al utilizar Internet: Caso Mérida-Venezuela.....	103
<i>Esly Lopez, Reinaldo Mayol Arnao and Solbey Morillo Puente</i>	

Un Framework para la Definición e Implantación de Mecanismos de Control de Acceso Basado en Roles, Contenidos e Información Contextual.....	112
<i>Gustavo Betarte, Andrés Gatto, Rodrigo Martínez and Felipe Zipitría</i>	
Identification Features For Users and Mobile Devices.....	122
<i>Israel Buitrón and Guillermo Morales</i>	
Security for WAP Provisioning Messages over TETRA Networks.....	126
<i>Joan Martínez</i>	
Facilitando la administración de la seguridad en tu red DMZ: MatFel.....	134
<i>Francisco Javier Díaz, Einar Lanfranco, Matías Pagano and Paula Venosa</i>	
U2-Route: Herramienta para el desarrollo de mecanismos de seguridad a nivel de Hardware.....	140
<i>Jhon Padilla, Luis Santamaria, Carlos Acevedo, Oscar Maestre and Line Becerra</i>	
Software de gestión para pruebas de penetración.....	146
<i>Carlos Noguera and Ronald Escalona</i>	
A Systematic Review of Security Patterns Used to Develop Security Architectures...	156
<i>Roberto Ortiz, Santiago Moral-Rubio, Javier Garzás and Eduardo Fernández-Medina</i>	
Metodología ágil de establecimiento de sistemas de gestión de la seguridad de la información basados en ISO/IEC27001.....	163
<i>Jeffrey Steve Borbon Sanabria and Erika Tatiana Luque Melo</i>	
Análisis de características de PDFs maliciosos.....	168
<i>Hugo Gonzalez</i>	
Análisis E Implementación De Las Técnicas Anti-Forenses Sobre ZFS.....	174
<i>Jonathan Cifuentes and Jeimy Cano</i>	
Cumplimiento de la LOPD y los requerimientos legales de la ISO27001 en la citación de pacientes en Hospitales.....	184
<i>Luis Enrique Sánchez Crespo, Antonio Santos-Olmo Parra, Esther Álvarez González, Eduardo Fernández-Medina Patón and Mario Piattini Velthuis</i>	
Primeros resultados de la encuesta de formación universitaria de grado en Seguridad de la Información en Iberoamérica.....	198
<i>Jorge Ramió Aguirre; Mari ángeles Mahillo García</i>	
Factores relevantes en el diseño de programas de posgrado en seguridad informática con calidad académica.....	206
<i>Angélica Flórez Abril</i>	
Asignatura de Protección y Seguridad de los Sistemas de Información orientada a su aplicación en negocios de Internet.....	213
<i>Luis Enrique Sánchez Crespo</i>	

Enseñanza del Método de Análisis y Recuperación de la Información haciendo uso de Herramientas de Software.....	219
<i>Francisco Nicolás Solarte Solarte; Edgar Rodrigo Enriquez Rosero</i>	
Experiencias en el uso de aulas virtuales como apoyo a la clase presencial de la asignatura de Criptografía.....	225
<i>Danilo Pástor Ramirez</i>	
Experiencias docentes para la enseñanza de la Seguridad informática en los programas de Ingeniería de sistemas.....	231
<i>Andrés Enríquez</i>	
Experiencia de implementación de la currícula de Seguridad Informática.....	236
<i>Hugo F. González Robledo</i>	
Seguridad en redes y aplicaciones distribuidas.....	242
<i>Carlos Eduardo Gómez Montoya</i>	
De la formación a la investigación en seguridad de la información.....	248
<i>Luis A. Solís</i>	
Evolución y Estado Actual de la Seguridad Informática y su Enseñanza en México.....	254
<i>Leobardo Hernández</i>	
Hacking ético en Debian Gnu/Linux, como escenario Integrador de prácticas en Seguridad informática.....	261
<i>Felipe Andrés Corredor Chavarro</i>	
GASTI – Un programa de Maestría orientado hacia las necesidades del Mercado Laboral Global.....	267
<i>Mauricio Vergara V.</i>	
Propuesta ética y fundamentación legal en la Cátedra de Seguridad Informática.....	273
<i>Luis Visley Aponte Cardona</i>	
Incorporación de contenidos de Seguridad y Auditoría en el Grado de Informática conforme a las certificaciones profesionales.....	279
<i>David García Rosado</i>	
Líneas de profundización en seguridad informática y su incorporación en el proceso de formación de los Ingenieros de Sistemas.....	285
<i>Fabián Castillo Peña</i>	

# Asignatura de Protección y Seguridad de los Sistemas de Información orientada a su aplicación en negocios de Internet

Primer Taller Iberoamericano de Enseñanza e Innovación Educativa en Seguridad de la Información TIBETS – Bucaramanga, Colombia, 3 de noviembre de 2011

Luis Enrique Sánchez Crespo  
GSyA. Universidad de Castilla-La Mancha



CRIPTORED

TIBETS 2011

por una mejor enseñanza de la Seguridad de la Información

- **Motivación**
  - Cambios en la sociedad asociados a las TIC
  - Auge de las nuevas tecnologías, en especial las relacionadas con internet.
  - Demanda de profesionales en seguridad y auditoría
  - Falta de cultura asociada a las nuevas tecnologías
  - Facilitar el acercamiento al concepto de seguridad en internet
  - Creciente importancia de la seguridad en internet.
  - Auge del mercado negro de tráfico de datos.

## • Objetivos

- Establecer una guía que permita a los alumnos entender como proteger de forma adecuada negocios en la red.
- Ayudar a los alumnos a entender la problemática que implica el cambio conceptual entre proteger algo físico frente a los sistemas virtuales.
- Conocer los riesgos asociados a los sistemas de internet.
- Entender como estos riesgos se incrementan al utilizar software libre.
- Conocer como mitigar estos riesgos y proteger de forma adecuada los negocios en la red.

## • Información de la asignatura de Protección y Seguridad de la Información

- Ingeniería Técnica en Informática de Sistemas
- Escuela Superior de Informática de Ciudad Real
- Universidad de Castilla-La Mancha, España
- Participantes: 1 profesor de la ESI
- Docencia: 3º
- Disciplinas: seguridad y auditoría, negocios en internet.
- Duración: 2ª Cuatrimestre

- **Temario:**

- *Tema 1* – Introducción a los conceptos de protección y seguridad en los sistema de Información.
- *Tema 2* – Gestión de la Seguridad – ISO27001.
- *Tema 3* – Fundamentos de la criptografía y gestión de las claves.
- *Tema 4* – Esquemas y protocolos de seguridad.
- *Tema 5* – Protección y Seguridad de Sistemas de Información.
- *Tema 6* – Protección y Seguridad de los negocios en internet.
- *Tema 7* - Protección y Seguridad del Software.

5

- **Competencias Genéricas y Específicas:**

- *G1* - Tener iniciativas positivas y mostrar compromiso ético en su comportamiento.
- *G2* - Capacidad de búsqueda, análisis e integración de información de una complejidad considerable.
- *G3* - Capacidad de influir positivamente en sus compañeros de equipo y trabajar satisfactoriamente para el mismo.
- *G4* - Haber distribuido el tiempo de estudio y trabajo eficientemente.
- *G5* - Ser capaz de leer y entender con soltura textos técnicos en castellano y en inglés.
- *G6* - Escribir textos bien estructurados y redactados.
- *G7* - Expresarse oralmente con claridad y coherencia.
- *E1* - Percibir la necesidad y justificación de la protección de la información, tanto almacenada como transmitida.
- *E2* - Aprender diferentes técnicas, procedimientos y herramientas de protección de los equipos y de las redes de comunicaciones.

6

- Planificación docente - dedicación:

Horas de esfuerzo durante el curso: 125 (5 x 25)				
	Presenciales		No presenciales	Total
	En aula	En laboratorio		
En semanas lectivas	33,5	12,5	58	104
En semanas no lectivas	4	0	17	21
<b>Total</b>	<b>37,5</b>	<b>12,5</b>	<b>75</b>	<b>125</b>

Distribución de horas semanales en semanas lectivas completas				
	Presenciales		No presenciales	Total
	En aula	En laboratorio		
Media	2,23	0,83	3,87	6,93
Máxima	5		5	8
Mínima	2		3	6

7

- Planificación docente – Actividades, competencias y organización temporal:

Actividades distribuidas a lo largo del curso	Competencias u otros objetivos de la actividad	Tiempo para su realización	N.º de créditos ECTS
Estudio y trabajo individuales	Todas las competencias	Todas las semanas.	1,6
Clases magistrales	E1, E2, G1, G2, G5, G7.	Todas las semanas.	0,7
Ejercicios y casos de estudio	Todas las competencias	Cuando se haya estudiado la materia que permite abordarlos	0,2
Tutorías docentes (clases de revisión, discusión, resolución de dudas, orientación de ejercicios)	E1, E2, G1, G2, G4, G5 y G7.	Cuando lo soliciten los alumnos, proceda corregir ejercicios u otras actividades o se avecine una prueba de evaluación	0,4
Tutorías individualizadas o para grupos pequeños	Todas las competencias	Cuando se produzca el reparto de trabajos y/o los alumnos lo soliciten	0,15
Prácticas de laboratorio	E1, E2, G1, G2, G4, G5, G6 y G7.	Cada dos semanas	0,5
Uso de Campus Virtual	Que los alumnos puedan encontrar la información que el profesor pone a su disposición así como realizar actividades de autoaprendizaje, etc. E1, E2, G1, G2, G2, G5.	Cuando el alumno desee o lo necesite	0,1

8

- Planificación docente – Actividades, competencias y organización temporal:

Actividades de aprendizaje localizadas en periodos determinados	Competencias u otros objetivos de la actividad	Tiempo para su realización	N.º de créditos ECTS
Búsqueda/Integración de Información	Que el estudiante sea capaz de buscar la información necesaria para la realización de los trabajos así como de integrarla de forma coherente. G5, G6	A partir de la semana 3 (trabajo individual), a partir de la semana 1 (trabajo en grupo)	0,45
Lecturas de textos técnicos	E1, E2, G1, G2, G3 y G5	Desde la semana 3 hasta la semana 6	
Realización trabajos en grupo	Todas las competencias	A partir de la semana 3 (trabajo individual), a partir de la semana 1 (trabajo en grupo)	0,5
Debate trabajos en grupo	E1, E2, G1, G2, G5, G7.	Semana 13 y 14	

9

- Planificación docente – Actividades, competencias y organización temporal:

Actividades de evaluación sumativa	Competencias u otros objetivos de la actividad	Tiempo para su realización	N.º de créditos ECTS
Exámenes de teoría y problemas	E1, E2, G1, G2, G3, G4, G5, G6.	Uno en el periodo ordinario de exámenes y otro en el periodo de exámenes extraordinarios.	0,4
Exámenes de laboratorio	E2, G1, G2, G3, G4, G5, G6 y G7.	Hacia las semanas 10, 12 y 14	
Entrega trabajos en individuales	Que el profesor evalúe los trabajos	Hacia la semana 5	
Entrega trabajos grupo	Que el profesor evalúe los trabajos	Hacia la semana 11	
Exposición de trabajos individuales	E2, G1, G2, G4, G6 y G7.	Hacia las semanas 5 y 6	
Exposición de trabajos en grupo	E1, E2, G1, G2, G4, G6 y G7.	Hacia las semanas 13 y 14	

10

- Planificación docente – Actividades, competencias y organización temporal:

Actividades de evaluación sumativa	Competencias u otros objetivos de la actividad	Tiempo para su realización	N.º de créditos ECTS
Exámenes de teoría y problemas	E1, E2, G1, G2, G3, G4, G5, G6.	Uno en el periodo ordinario de exámenes y otro en el periodo de exámenes extraordinarios.	0,4
Exámenes de laboratorio	E2, G1, G2, G3, G4, G5, G6 y G7.	Hacia las semanas 10, 12 y 14	
Entrega trabajos en individuales	Que el profesor evalúe los trabajos	Hacia la semana 5	
Entrega trabajos grupo	Que el profesor evalúe los trabajos	Hacia la semana 11	
Exposición de trabajos individuales	E2, G1, G2, G4, G6 y G7.	Hacia las semanas 5 y 6	
Exposición de trabajos en grupo	E1, E2, G1, G2, G4, G6 y G7.	Hacia las semanas 13 y 14	

11

- Conclusiones

- Los alumnos que vayan a trabajar con sistemas de información, y en especial cuando estos se encuentran en internet y han sido desarrollados utilizando software libre, deben:
  - Conocer el problema psicológico y social que supone el cambio de paradigma de seguridad sobre objetos físicos vs seguridad en entornos virtuales.
  - Conocer como podemos proteger y gestionar la seguridad en: Sistemas de Información clásicos, software y negocios de internet.
  - Conocer como los hackers se aprovechan de los agujeros de seguridad de las aplicaciones Open Source.