

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>	

Incorporación de contenidos de Seguridad y Auditoría en el Grado de Informática conforme a las certificaciones profesionales

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

David García Rosado
GSyA. Universidad de Castilla-La Mancha



CRIPTORED

TIBETS 2011

per una mejor enseñanza de la Seguridad de la Información

- Motivación
 - Adaptación de los estudios de Informática al EEES
 - Auge de las nuevas tecnologías
 - Demanda de profesionales en seguridad y auditoría
 - Nuevos estudios estén muy enfocados a las necesidades profesionales
 - Facilitar el acercamiento hacia las certificaciones profesionales
 - Proponer y recomendar contenidos de Seguridad y Auditoría
 - Competencias y objetivos de asignaturas
 - Encaminadas a las necesidades reales de la industria
 - Bien acopladas, encajadas, ajustadas y coordinadas

• Objetivos

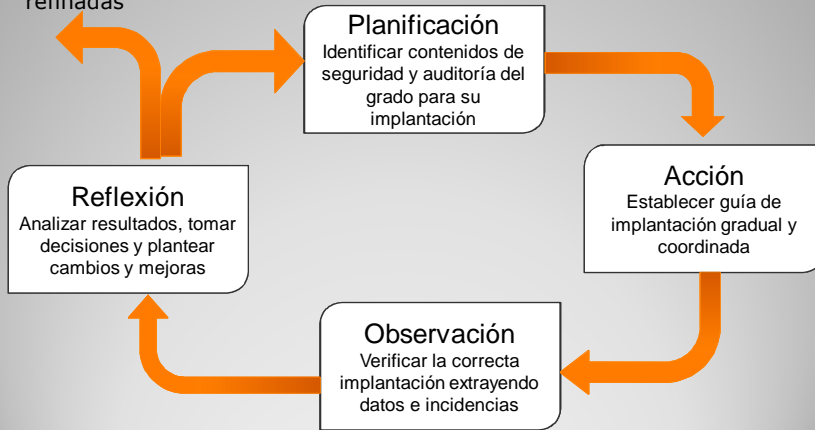
- Establecer una guía transversal para la implantación de contenidos relacionados con la seguridad informática
- Contenidos bien definidos y orquestados
- En los tres primeros cursos, el alumno adquiere los conocimientos básicos de seguridad
- Un futuro graduado en Informática tendrá
 - las nociones y conocimientos básicos sobre Seguridad,
 - amplios conocimientos sobre un área en concreto
 - las bases necesarias para optar a alguna de las acreditaciones profesionales de seguridad.

• Información del proyecto de innovación

- Grado en Ingeniería Informática
- Escuela Superior de Informática de Ciudad Real
- Universidad de Castilla-La Mancha, España
- Participantes: 13 profesores de la ESI
- Docencia: en todos los cursos
- Disciplinas: seguridad y auditoría, gestión de proyectos, gestión del conocimiento, bases de datos, sistemas de información, etc.
- Duración: Octubre a Septiembre (12 meses)

• Metodología Aplicada

Soluciones refinadas



5

• Actividades

1 Coordinación

- Un informe de seguimiento que nos indique cómo se está desarrollando el proyecto

2 Análisis de las certificaciones profesionales

- La lista de contenidos de seguridad y auditoría, extraídos de las principales certificaciones profesionales

3 Análisis de las asignaturas del grado

- La lista de asignaturas del grado que son candidatas a ser actualizadas y/o modificadas

4 Establecer guía de implantación

- Una guía de implantación en el grado

5 Definir mapas de conocimiento orientados a certificaciones

- Mapas de conocimientos orientados a las certificaciones profesionales

• Resultados

Un informe de seguimiento que nos indique cómo se está desarrollando el proyecto

- Documento donde se indica
 - cuál ha sido la evolución del proyecto
 - quienes son los implicados,
 - qué se debe presentar
 - qué queda por hacer, aclarando plazos y coordinación entre todos
 - definiendo los hitos futuros
 - aclarar dudas
 - ver el estado actual del proyecto.

• Resultados

La lista de contenidos de seguridad y auditoría, extraídos de las principales certificaciones profesionales

CISA (Certified Information System Auditor)	CIA (Certified Internal Auditor)
CISM (Certified Information Security Manager)	CIPP (Certified Information Privacy Professional)
CISSP (Certified Information System Security Manager)	CPP (Certified Protection Professional)
GIAC (Global Information Security Assurance Certification)	CCSP (Cisco Certified Security Professional)
Auditoría de sistemas de información	Seguridad en el Desarrollo de Aplicaciones y Sistemas
Auditoría de sistemas de información	Seguridad en el Desarrollo de Aplicaciones y Sistemas
Gobierno y gestión de TI	Criptografía
Gestión de riesgos de la información	Seguridad Física
Desarrollo del programa de seguridad de información	Seguridad en Internet, Redes y Telecomunicaciones
Arquitectura y Modelos de Seguridad	Recuperación ante Desastres y Planificación de la Continuidad del Negocio
Sistemas y Metodología de Control de Acceso	Leyes, investigaciones y Ética

Resultados

La lista de asignaturas del grado que son candidatas a ser actualizadas y/o modificada

Administración de Bases de Datos	Desarrollo de Bases de Datos	Redes de Computadores II
Análisis Forense Informático	Desarrollo de Sistemas Web	Redes y Servicios Móviles
Aplicaciones Distribuidas en Internet	Diseño y Gestión de Redes	Seguridad de los Sistemas Informáticos
Arquitectura de Computadores	Gestión de proyectos Software	Seguridad de Sistemas Software
Aspectos Profesionales de la Informática	Gestión de Sistemas de Información	Seguridad en redes
Auditoría en Sistemas de Información	Gestión y Administración de redes	Sistemas Distribuidos
Bases de Datos	Ingeniería de Negocio	Sistemas Operativos I
Bases de Datos Avanzadas	Ingeniería de Requisitos	Tecnologías y Sistemas Web
Cálculo y Métodos Numéricos	Ingeniería del Software II	
Comercio electrónico	Multimedia	

Resultados

Una guía de implantación

	ARQ	AUD	CON	CRI	DAP	FIS	GOB	INT	LEY	NEG	PRO	RIE
Gestión de Sistemas de Información												
Gestión y Administración de redes												
Ingeniería de Negocio												
Ingeniería de Requisitos												
Ingeniería del Software II												
Multimedia												
Redes de Computadores II												
Redes y Servicios Móviles												
Seguridad de los Sistemas Informáticos												
Seguridad de Sistemas Software												
Seguridad en redes												
Sistemas Distribuidos												
Sistemas Operativos I												
Tecnologías y Sistemas Web												

Resultados

Mapas de conocimientos orientadas a las certificaciones profesionales

		CISA	CISM	CISSP	GIAC	CIA	CIPP	CPP	CCSP	
4º	IS	Gestión de Proyectos Software								
		Desarrollo de Bases de Datos								
		Sistemas de Información Empresariales								
		Seguridad de Sistemas Software								
	IC	Seguridad en Redes								
		Planificación e Integración de Sistemas y Servicios								
		Gestión y Administración de Redes								
		Diseño de Infraestructura de Red								
	7º	CO	Sistemas basados en el Conocimiento							
			Diseño de Sistemas Interactivos							
	TI	Opt	Minería de Datos							
			Programación Declarativa							
		Opt	Tecnologías y Sistemas Web							
			Comercio Electrónico							
		Opt	Multimedia							
			Seguridad en Sistemas Informáticos							
		8º	Opt	Ingeniería de Negocio						
				Bases de Datos Avanzadas						
			Opt	Auditoría de Sistemas de Información						
				Administración de Bases de Datos						
Opt	Desarrollo de Sistemas Web									
	Análisis Forense Informático									
Opt	Redes y Servicios Móviles									
Opt	Aplicaciones Distribuidas en Internet									

Conclusiones

- Los contenidos de seguridad y auditoría dentro del grado en Ingeniería Informática deben
 - estar perfectamente acoplados y organizados de forma que sea una progresión de conocimientos conforme se vaya avanzando en el grado
 - tengan una relación directa entre contenidos
 - estén ajustados a las competencias y objetivos de las asignaturas
 - estén orientados a las necesidades más demandadas por la sociedad.