DEPARTAMENTO DE
INFORMÁTICA

Universidad Técnica Federico Santa María

Contacto

CIBSI´05
Departamento de Informática - UTFSM
Casilla 110-V
Valparaíso - Chile

Fono: +56(32) 654 429
Fono: +56(32) 654 424
Fax: +56(32) 797 513
e-mail: cibsi@inf.utfsm.cl
cibsi05@inf.utfsm.cl
URL:http://cibsi05.inf.utfsm.cl

≫AUSPICIA

Microsoft · software AG · IBM · McAfee · Cisco Systems · Impsat · mti · GALA · Grami · NEOSECURE · ORACLE · Guidance Software

≫PATRONCINA

Biblioteca del Congreso Nacional de Chile · Corporación de Capacitación y Empleo SOFOFA · Sociedad Chilena de Ciencia de la computación

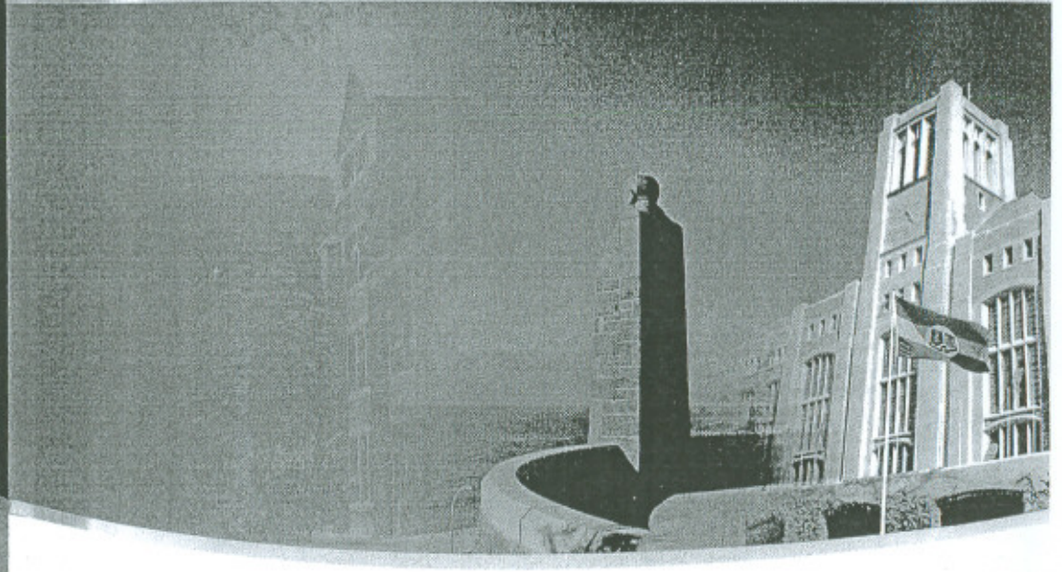
UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

UNIVERSIDAD TECNICA FEDERICO SANTA MARIA
DEPARTAMENTO DE INFORMATICA

3ER CONGRESO IBEROAMERICANO DE SEGURIDAD INFORMATICA

DEPARTAMENTO DE INFORMÁTICA

CIBSI05



21-25 NOVIEMBRE 2005

ACTAS

CONGRESO IBEROAMERICANO DE SEGURIDAD INFORMATICA

21 - 25 de Noviembre de 2005

Valparaíso, Chile

ISBN 956-7051-10-0
Actas del
3° Congreso Iberoamericano de Seguridad Informática

CIBSI'05

Prólogo

Tenemos el agrado de poner a disposición de los participantes los trabajos aceptados y presentados en el **Tercer Congreso Iberoamericano de Seguridad Informática (CIBSI'05)** realizado entre el 21 y el 25 de Noviembre del 2005 en la ciudad de Valparaíso, Chile, evento que ha sido organizado por el Departamento de Informática de la Universidad Técnica Federico Santa María (Chile) en conjunto con la Universidad Politécnica de Madrid (España).

De un total de 60 artículos enviados al congreso, se seleccionaron un total de 35 trabajos. De este total, 31 de ellos tenían autores de un solo país, y que se distribuyen de la siguiente manera: Argentina (6), Brasil (2), Colombia (3), Chile (1), España (14), México (4) y Uruguay (1). Además se presentaron otros 4 trabajos con autores de diferentes países, donde en cada uno de ellos al menos existe un coautor español y los demás coautores son de Chile, EE.UU., Francia, Polonia y Uruguay.

Los artículos seleccionados cubren las áreas:

- Criptografía, esteganografía y protocolos de seguridad.
- Seguridad en sistemas, redes, comunicaciones y prevención y detección de intrusos.
- Seguridad en sistemas de información, en la Web y en el comercio electrónico
- Modelos de gestión y auditoría en seguridad

Como parte del programa se han incluido tres charlas magistrales sobre voto electrónico, seguridad en entornos ubicuos y tendencias en criptografía.

También como parte del programa, se organizó en conjunto con la Biblioteca del Congreso Nacional de Chile, en el primer día, un evento sobre seguridad informática en el Estado y se incluyeron 5 charlas técnicas de empresas auspiciadoras tales como Cisco Systems, IBM, McCaffee, Neosecure y Software AG.

Deseamos agradecer primero al Comité de Programa por el esfuerzo realizado en la revisión de todos los artículos y en el proceso de selección de éstos. En segundo lugar agradecer a los patrocinadores y auspiciadores que apoyaron de diferentes formas a producir el evento CIBSI'05. Finalmente agradecer a todos los organizadores. Esperamos que la estadía en Valparaíso y la participación en CIBSI'05 haya sido provechosa y de su agrado.

Raúl Monge
Presidente de Comité Organizador

Jorge Ramió
Vicepresidente de Comité Organizador

Valparaíso, Chile

Noviembre, 2005

Organización

Comité Organizador

Dr. Raúl Monge Anwandter (Universidad Técnica Federico Santa María, Chile)
Dr. Jorge Ramió Aguirre (Universidad Politécnica de Madrid, España)
Sr. Javier Cañas Robles (Universidad Técnica Federico Santa María, Chile)

Conferencistas Invitados

Dr. René Peralta (National Institute of Standards and Technology, USA)
Dr. Javier López (Universidad de Málaga, España)

Comité de Programa

Dr. Juan Pedro Hecht (Universidad de Buenos Aires, Argentina)
Dr. Hugo Scolnik (Universidad de Buenos Aires, Argentina)
Dr. Ricardo Dahab (Universidade Estadual de Campinas, Brasil)
Dr. Marco Aurelio Henriques (Universidade Estadual de Campinas, Brasil)
Dr. Adriano Mauro Cansian (Universidade Estadual Paulista, Brasil)
Dr. Routo Terada (Universidade de São Paulo, Brasil)
Dr. Marcos Kiwi (Universidad de Chile, Chile)
Dr. Horst von Brand (Universidad Técnica Federico Santa María, Chile)
Dr. Juan Guillermo Lalinde Pulido (Universidad EAFIT, Colombia)
Dr. Jeimy José Cano Martínez (Universidad de los Andes, Colombia)
Dr. Julio Cesar López (Universidad del Valle, Colombia)
Dr. Jorge Estrada Sarlabous (Academia de Ciencias de Cuba, Cuba)
Dr. Javier Areito Bertolín (Universidad de Deusto, España)
Dr. Joan Borrel Viader (Universidad Autónoma de Barcelona, España)
Dra. Pino Caballero Gil (Universidad de La Laguna, España)
Dr. Jorge Dávila Muro (Universidad Politécnica de Madrid, España)
Dr. Luis Hernández Encinas (Consejo Superior de Investigaciones Cientificas CSIC, España)
Dr. Josep Lluis Ferrer-Gomila (Universidad de Las Islas Baleares, España)
Dr. Francisco Javier López Muñoz (Universidad de Málaga, España)
Dra. Amparo Fúster Sabater (Consejo Superior de Investigaciones Cientificas CSIC, España)
Dr. Arturo Ribagorda Garnacho (Universidad Carlos III de Madrid, España)
Dr. Miguel Soriano Ibañéz (Universidad Politécnica de Cataluña, España)
Dr. Hugo César Coyote Estrada (Instituto Politécnico Nacional, México)
Dr. Enrique Daltabuit Godas (Universidad Nacional Autónoma de México, México)
Dr. Carlos Mex Perera (ITESM campus Monterrey, México)

Dr. Sergio Rajsbaum Godorezky (Universidad Nacional Autónoma de México, México)
Dr. Horacio Tapia Recillas (Universidad Autónoma Metropolitana, México)
Dr. Edmundo Monteiro (Universidad de Coimbra, Portugal)
Dr. Emilio Hernández (Universidad Simón Bolívar, Venezuela)
Dr. Alfredo Viola Deambrosis (Universidad de la República - Uruguay)

Logística

Srta. Claudia Arancibia (Universidad Técnica Federico Santa María, Chile)
Srta. Carol Castro (Universidad Técnica Federico Santa María, Chile)

Edición y Publicación de Actas

Sr. Pablo Itaim (Universidad Técnica Federico Santa María, Chile)

Auspician

Patrocinan

Índice general

Prólogo 3

Organización 4

Comité de Programa 5

Índice General 7

Conferencias Magistrales

Martes, 22 de Noviembre 2005, 12:45-14:00

Tecnologías de Voto electrónico 13
Dr. René Peralta, National Institute of Standards and Technology (EE.UU.)

Miércoles, 23 de Noviembre 2005, 12:45-14:00

Entornos pervasivos y ubicuos: La nueva (in)-seguridad 13
Dr. Javier López (Universidad de Málaga, España)

Programa Técnico

Martes 22 de Noviembre del 2005, 11:00-12:30

SESIÓN N°1: Seguridad en Comercio Electrónico

Tarjetas de crédito anónimas con pago sin conexión 17
Álvarez Manuel, Universidad Politécnica de Madrid (España)
Carracedo Justo, Universidad Politécnica de Madrid (España)

Implementación de un Monedero Electrónico Seguro Sobre el Análisis del Protocolo SET ... 31
Lizama Luis, Universidad Juárez Autónoma de Tabasco (México)
León Roberto, Universidad Juárez Autónoma de Tabasco (México) (2)

Alternativa de solución aplicada al esquema de micropago electrónico MR3 45
Gallegos Gina, Escuela Superior de Ingeniería Mecánica y Eléctrica Unidad Culhuacán (México)
Vázquez Rubén, Escuela Superior de Ingeniería Mecánica y Eléctrica Unidad Culhuacán (México)
Salinas Moisés, Escuela Superior de Ingeniería Mecánica y Eléctrica Unidad Culhuacán (México)

Martes 22 de Noviembre del 2005, 15:00 – 16:30 horas

SESIÓN N°2: Votaciones Electrónicas y Privacidad de la Información

Un Protocolo de Votación y Recuento en Elecciones Electrónicas 63
Abascal P. , Universidad de Oviedo (España)
Tena J., Universidad de Valladolid (España)

Diseño de un sistema avanzado de democracia digital garante de la libertad de Expresión ... 75
Gómez Ana, Universidad Politécnica de Madrid (España)
Pérez Emilia, Universidad Politécnica de Madrid (España)
Sánchez Sergio, Universidad Politécnica de Madrid (España)
Moreno Jesús, Universidad Politécnica de Madrid (España)
González Carlos, Universidad Politécnica de Madrid (España)

Legislación y Técnicas para preservar la Privacidad de la Información Espacio-Temporal (PIET) ... 91
Ramos Benjamin, Universidad Carlos III de Madrid (España)
González-Tablas Ana, Universidad Carlos III de Madrid (España)
Ribagorda Arturo, Universidad Carlos III de Madrid (España)

Miércoles 23 de Noviembre del 2005, 09:00 – 10:30 horas

SESIÓN N°3: Criptografía I

A provably secure crypto-compression algorithm ... 107
Milidiú Ruy, Informatics Department of PUC-Rio (Brasil)
Mello Claudio, Military Institute of Engineering (IME) (Brasil)

Computing Tate Pairing for some Large Characteristic Fields ... 123
Ángel José, Computer Science, CINVESTAV-IPN (México)
Morales-Luna Guillermo, Computer Science, CINVESTAV-IPN (México)

A study of 3 by 3 S-boxes and its application on a bitsliced multiplicative cipher: Quetzalcoatl ... 133
Fontana Sebastián, Universidad Nacional de Córdoba (Argentina)
Penazzi Daniel, Universidad Nacional de Córdoba (Argentina)

Miércoles 23 de Noviembre del 2005, 11:00 – 12:30 horas

SESIÓN N°4: Criptografía II

Variante del criptosistema de Meyer-Müller con triplicado de puntos ... 151
Martínez S., Universitat de Lleida (España)
Miret J., Universitat de Lleida (España)
Moreno R., Universitat de Lleida (España)
Tomas R., Universitat de Lleida (España)
Valls M., Universitat de Lleida (España)

A Survey of Cryptographic Libraries Supporting Elliptic Curve Cryptography ... 159
Reis Jr. David, CPqD Telecom & IT Solutions (Brasil)
Uto Nelson, CPqD Telecom & IT Solutions (Brasil)

Revisión crítica de los ataques de colisiones diferenciales contra las funciones hashing de la familia MD4 ... 177
Hecht Juan, Universidad de Buenos Aires (Argentina)
Scolnik Hugo, Universidad de Buenos Aires (Argentina)

Miércoles 23 de Noviembre del 2005, 15:00 – 16:30 horas

SESIÓN N°5: Criptografía y Esteganografía

Caos Discreto y Criptografía ... 193
Amigó José, Universidad Miguel Hernández (España)
Szczepanski Janusz, Polish Academy of Science (Polonia)
Kocarev Ljupco, University of California San Diego (EE.UU.)

Criptografía caótica con reinyección de la información ... 207
Millérioux Gilles, Université Henri Poincaré (Francia)
Hernández Adrián, Universidad Miguel Hernández (España)
Amigó José, Universidad Miguel Hernández (España)

Espectro Disperso para Canales Subliminales Esteganográficos (CSE) ... 221
Ortega-Laurel C., Instituto Politécnico Nacional (México)
Vázquez-Medina R., Instituto Politécnico Nacional (México)
Cruz-Irison M., Instituto Politécnico Nacional (México)
Valverde-Domínguez R., Instituto Politécnico Nacional (México)

Jueves 24 de Noviembre del 2005, 09:00 – 10:30 horas

SESIÓN N°6: Protocolos de Seguridad

Autenticación mediante Verificación del Locutor ... 233
Santos Verónica, Universidad Nacional del Comahue (Argentina)
Martín Daniel, Universidad Nacional del Comahue (Argentina)
Bertogna, Leandro, Universidad Nacional del Comahue (Argentina)
Sznek Jorge, Universidad Nacional del Comahue (Argentina)

Un nuevo esquema para el reparto de múltiples secretos ... 247
Álvarez G. , IFA, CSIC (España)
Hernández L., IFA, CSIC (España)
Martín A., Universidad de Salamanca (España)
Ramió Jorge, Universidad Politécnica de Madrid (España)

Protocolos de sellado espacio-temporal: Mejorando su precisión y disminuyendo el nivel de confianza requerido ... 259
González-Tablas Ana, Universidad Carlos III de Madrid (España)
Ramos Benjamín, Universidad Carlos III de Madrid (España)
Ribagorda Arturo, Universidad Carlos III de Madrid (España)

Jueves 24 de Noviembre del 2005, 11:00 – 12:30 horas

SESIÓN N°7: Seguridad en Redes y Comunicaciones

Análisis del impacto en la homogeneidad de recursos de las redes ad-hoc con autoridad de certificación distribuida ... 275
Azuara Guillermo, Universidad de Zaragoza (España)
Salazar José, Universidad de Zaragoza (España)

Una técnica de protección para agentes móviles contra estaciones (hosts) maliciosas 289
Waissbein Ariel, Core Security Technologies (Argentina)

Modelo de Ataques y riesgo residual para desbordamientos de Buffer 301
Álvarez Juan, Fluidsignal Group (Colombia)
Lalinde-Pulido Juan, Universidad EAFIT (Colombia)

Jueves 24 de Noviembre del 2005, 12:45 – 13:45 horas

SESIÓN N°8: Prevención y Detección de Intrusos

Sistema inteligente para la prevención de intrusos y ataques en redes de información clínica descentralizada 319
Gago Esther, Universidad Politécnica de Madrid (España)
Pau de la Cruz Iván, Universidad Politécnica de Madrid (España)
Valero Miguel, Universidad Politécnica de Madrid (España)

Sistema de Detección de Intrusos Basado en un Análisis Probabilística del Comportamiento del Usuario 335
González Roberto, Universidad de Santiago de Chile (Chile)
Figueroa German, Universidad de Santiago de Chile (Chile)
Pinacho Pedro, Universidad de Santiago de Chile (Chile)

Jueves 24 de Noviembre del 2005, 15:00 – 16:30 horas

SESIÓN N°9: Seguridad en la Web

Preventing and Handling Phishing Attacks 353
Echaiz Javier, Universidad Nacional del Sur (Argentina)
Ardenghi Jorge, Universidad Nacional del Sur (Argentina)

Ataques Web Automáticos: Identificación, Engaño y Contraataque 369
Nuñez Mariano, CYBSEC Security Systems (Argentina)

Elicitación de Requisitos de Seguridad para Servicios Web en PWSSec 385
Gutiérrez Carlos, Universidad de Castilla-La Mancha (España)
Fernández-Medina Eduardo, Universidad Castilla-La Mancha (España)
Piattini Mario, Universidad Castilla-La Mancha (España)

Viernes 25 de Noviembre del 2005, 09:00 – 10:30 horas

SESIÓN N°10: Modelos de Gestión de la Seguridad de Información

Sistemas de Seguridad de la Información. Un enfoque "Sistémico" 401
Rodríguez Manuel, Ministerio de Economía y Hacienda de España (España)
Ramos Benjamín, Universidad Carlos III de Madrid (España)

Hacia un Modelo de Gestión de Seguridad de la Información para Pequeñas y Mediana Empresa con la ISO/IEC 17799 415
Villafranca Daniel, SICAMAN Nuevas Tecnologías (España)
Sánchez Luis, SICAMAN Nuevas Tecnologías (España)
Fernández-Medina Eduardo, Universidad Castilla-La Mancha (España)
Piattini Mario, Universidad Castilla-La Mancha (España)

Hacia un Modelo de Madurez para la Seguridad de la Información 429
Areiza Karen, Universidad EAFIT (Colombia)
Barrientos Andrea, Universidad EAFIT (Colombia)
Rincón Rafael, Universidad EAFIT (Colombia)
Lalinde-Pulido Juan, Universidad EAFIT (Colombia)

Viernes 25 de Noviembre del 2005, 11:00 – 12:30 horas

SESIÓN N°11: Seguridad en Sistemas de Información

Hacia la definición de Procesos de Negocios Seguros basados en una Arquitectura Dirigida por Modelos 443
Rodríguez Alfonso, Universidad del Bio Bio (Chile)
Fernández-Medina Eduardo, Universidad Castilla-La Mancha (España)
Piattini Mario, Universidad Castilla-La Mancha (España)

Hacia una Implementación Exitosa de un SGSI 457
Corti María, Universidad de la República (Uruguay)
Betarte Gustavo, Universidad de la República (Uruguay)
de la Fuente Reynaldo, Datasec (Uruguay)

Restricciones de Autorización en Sistemas de Gerenciamiento de Workflow 473
Moreno Juan, Universidad Católica del Uruguay (Uruguay)
Sorondo Peyre Martín, Universidad Católica del Uruguay (Uruguay)
Joyanes Luis, Universidad Pontificia de Salamanca (España)

Viernes 25 de Noviembre del 2005, 15:00 – 16:30 horas

SESIÓN N°12: Auditoría y Seguridad

La auditoría de sistemas de información y la tutela pública de la intimidad y la privacidad de las personas 491
Miralles Ramón, Agencia Catalana de Protección de Datos (España)
Vila Angels, Agencia Catalana de Protección de Datos (España)

La Norma Como Instrumento de Ayuda a la Mejora de la Seguridad: Un Ejemplo Práctico de Auditoría 509
Aced Emilio, Agencia de Protección de Datos de la Comunidad de Madrid (España)

Herramientas utilizadas para la auditoría de la eficiencia funcional de las aplicaciones informáticas, una visión actual 523
Riascos Sandra, Universidad Mariana (Colombia)

Índice de Autores 539
Relación por País 543
Relación de Títulos 547

Conferencias Magistrales

Tecnologías de voto electrónico

Martes, 22 de Noviembre 2005, 12:45-14:00

Dr. René Peralta
National Institute of Standards and Technology, USA

Se describirán, en líneas generales, las principales técnicas propuestas que existen hoy en día (algunas ya en uso) para voto electrónico. En EE.UU. existen actualmente dos fuertes controversias con respecto a esta tecnología. El primer punto en discusión es la conveniencia o no de generar, para efectos de auditoría, una copia en papel de cada voto. El segundo punto es la factibilidad del voto por Internet. Se presentarán los principales argumentos en pro y en contra de estas alternativas. Luego se muestra la posición del conferencista al respecto.

Entornos pervasivos y ubicuos: La nueva (in)-seguridad

Miércoles, 23 de Noviembre 2005, 12:45-14:00

Dr. Javier López
Universidad de Málaga, España

Como evolución a las aplicaciones desarrolladas para entornos móviles, las aplicaciones para entornos pervasivos y ubicuos se han establecido firmemente como la próxima frontera en la investigación de Seguridad. Parece obvio que las soluciones de seguridad desarrolladas para la tecnología de hace unos pocos años no resultan adecuadas, dadas las restrictivas características físicas de los nuevos dispositivos y los característicos entornos donde se usan. Aún así, el diseño de las nuevas soluciones preservan muchas de las características de antes, lo que supone un error en multitud de ocasiones. En esta presentación se analizarán los problemas que están abiertos y el abanico de posibles estrategias a seguir para dotar de soluciones seguras a estos nuevos entornos tecnológicos.

- McGraw G., IEEE Computer 32(4), pp. 103-105. "*Software Assurance for Security*", april, 1999.
- Métrica v3, *Metodología de Planificación, Desarrollo y Mantenimiento de Sistemas de Información*. Consejo Superior de Informática y para el Impulso de la Administración Electrónica, 2000.
- Ministerio de Administraciones Públicas, "*Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*", MAP, versión 1.0, 1997.
- NIST Special Publication 800-64, "*Security Considerations in the Information System Development Life Cycle*", Rev.1. June 2004.
- NIST Special Publication 800-27 Rev. A, "*Engineering Principles for Information Technology Security (A Baseline for Achieving Security)*", Rev. A, June 2004.
- Robinson B., "*Making Software NASA Tough*", Federal Computer Week, July 1, 2002.
- Stallings W. , "*Introduction Cryptography and network security: principles and practice. Chapter 1, 2nd Ed*", Edit. Prentice Hall New Jersey (USA),1999.
- UNE-ISO/IEC 17799:2002, "*Tecnología de la Información. Código de Buenas Prácticas de la Gestión de la Seguridad de la Información*", 2002.
- United States General Accounting Office, Accounting and Information Management Division, "*Information Security Risk Assessment -- GAO Practices of Leading Organizations*".

Hacia un Modelo de Gestión de Seguridad de la Información para la Pequeña y Mediana Empresa con la ISO/IEC 17799

Daniel Villafranca[1], Luís Enrique Sánchez[1], Eduardo Fernández-Medina[2] y Mario Piattini[2]

[1]SICAMAN Nuevas Tecnologías. Departamento de I+D,
Juan José Rodrigo, 4. Tomelloso, Ciudad Real, España.
{dvillafranca, lesanchez} @sicaman-nt.com
[2] Universidad Castilla-La Mancha, Grupo de Investigación Alarcos, Departamento de Tecnologías y Sistemas de Información,
Paseo de la Universidad 4, Ciudad Real, España.
{Eduardo.FdezMedina, Mario.Piattini}@uclm.es

Resumen. Para que las empresas puedan utilizar las tecnologías de la información y las comunicaciones con garantías, es necesario disponer de guías, métricas y herramientas que nos permitan conocer en cada momento el nivel de nuestra seguridad y los puntos que no estamos cubriendo en la misma. En las pequeñas y medianas empresas, la aplicación de normativas de seguridad cuenta con el problema adicional de no tener recursos suficientes para realizar una adecuada gestión. En este artículo mostramos un nuevo enfoque para gestionar la seguridad de este tipo de empresas, adaptado al tamaño de la empresa y a su nivel de madurez, utilizando como marco de referencia la norma ISO/IEC 17799. Este enfoque está siendo aplicado directamente a casos reales, consiguiendo así una constante mejora en su aplicación.

1 Introducción

La información y los procesos que apoyan los sistemas y las redes son los activos más importantes para cualquier organización [1]. Estos activos están sometidos a riesgos de una gran variedad, que pueden afectar de forma crítica a la empresa.

El cambio social producido por Internet y la rapidez en el intercambio de información, ha producido que las empresas empiecen a tomar conciencia del valor que tiene la información para sus organizaciones y se preocupen de proteger sus datos.

El nuevo modelo empresarial que comenzó a implantase a principios de siglo, y que estaba basado en la implantación de sistemas de información, ha demostrado tener enormes beneficios para aumentar el nivel de competitividad de las empresas, y se ha convertido en el activo de mayor valor para la compañía y por tanto en el más importante desde el punto de vista de la seguridad. Para proteger estos sistemas de información, que representaban el principal factor diferenciador con respecto a su competencia, algunas empresas acometieron proyectos de implantación de sistemas

de seguridad basados en la instalación de controles puntuales. Éstos solucionaban aspectos puntuales de la seguridad, pero no incluían la gestión de dichos controles, ni un marco de gestión global de la seguridad que permitiera su estabilidad a medio y largo plazo. Con el tiempo, al no disponer de una gestión adecuada, esos controles dejaban de mantenerse y se convertían en controles pasivos, que en lugar de ayudar a mejorar la seguridad contribuían a crear una falsa sensación de seguridad. Así, en Tsujii [2] se destacaba que para la construcción de un sistema de seguridad no bastan los aspectos tecnológicos, sino que también son necesarios los aspectos de gestión, así como los aspectos legales y éticos.

Una vez que las empresas han empezado a tener una concienciación mínima en materia de seguridad, se encuentran con que no saben cómo securizar sus sistemas de información. La mayor parte de las empresas tienen sistemas de seguridad caóticos, creados sin unas guías adecuadas, sin documentación y con recursos insuficientes. Los controles clásicos se muestran por sí solos insuficientes para dar unas mínimas garantías de seguridad; las herramientas de seguridad existentes en el mercado ayudan a solucionar parte de los problemas de seguridad, pero nunca afrontan el problema de una manera global e integrada; por último, la enorme diversidad de estas herramientas y su falta de integración suponen un enorme coste en recursos para poderlas gestionar. Algunas cifras que nos muestran la magnitud de los problemas ocasionados por falta de unas medidas de seguridad adecuadas aparecen, por ejemplo, en [3], indicando que sobre una muestra de 257 empresas, el 90% de las empresas detectó fallos de seguridad, el 70% fueron fallos graves de seguridad (robo de portátiles, robo de información, fraude financiero, acceso al sistema por intrusos, sabotaje de datos o redes) y el 74% reconocieron pérdidas financieras debido a fallos de la seguridad. Otros informes aseguran que las pérdidas totales en los Estados Unidos en 2004 como resultado de fallos de seguridad en los ordenadores alcanzaron los $141.496.560.

A pesar de lo negativas que resultan las cifras anteriores, la situación es mucho más dramática en muchos países de Europa, y sobre todo en América Latina.

El mercado demanda actualmente a las empresas que sean capaces de garantizar que las tecnologías para los activos informáticos y de información sean seguras, rápidas y de fácil interacción. Pero para cumplir estos objetivos, los gerentes de sistemas se han encontrado con dos problemas para los que no existe una solución satisfactoria: la falta de herramientas que permitan afrontar la gestión de la seguridad de los sistemas de información de una forma centralizada, sencilla y dimensionada al tamaño de las compañías, y la falta de guías de seguridad de la información, que permitan responder a las preguntas de ¿dónde tengo que buscar?, ¿que tengo que controlar? y ¿cómo tengo que controlarlo?.

El primer problema sigue sin resolverse, pero creemos que podrá ser resuelto cuando se dé solución al segundo. Con respecto al segundo problema, las organizaciones tanto nacionales como internacionales se han preocupado por elaborar un conjunto de normas y especificaciones relativas a la seguridad en las tecnologías de la información y las comunicaciones. Éstas se centran sobre todo en la definición de controles de seguridad mediante códigos de buenas prácticas, normas que definen sistemas de gestión de seguridad, y normas con criterios para certificar la seguridad. No obstante, el panorama es complejo y, para una pequeña o mediana empresa, abordar la implantación de un sistema de gestión de seguridad, con la posibilidad de tener varios niveles de exigencia y con unos recursos limitados, se convierte en una

tarea muy compleja. Además, el proceso casi siempre termina derivando en que la empresa asuma el riesgo de carecer de un sistema de gestión de la seguridad, ante la incapacidad de implantarlo.

En este artículo presentamos una aproximación a la implantación de sistemas de gestión de seguridad, basado en la norma ISO/IEC 17799, que estamos desarrollando y mejorando continuamente gracias a la retroalimentación recibida directamente de los clientes de SICAMAN.

El artículo continúa en la Sección 2, describiendo brevemente el concepto de sistema de gestión de seguridad. En la Sección 3 se introduce el esquema de implantación de sistemas de gestión con las novedades que estamos aplicando, a nivel de metodología y software. Finalmente, en la Sección 4 concluimos indicando cuál será el trabajo que desarrollaremos en el futuro.

2 Los Sistemas de Gestión de Seguridad de la Información

Un sistema de Gestión de la seguridad de la información (SGSI) se puede definir como un sistema de Gestión usado para establecer y mantener un entorno seguro de la información. Este SGSI debe tratar la puesta en práctica y el mantenimiento de procesos y de procedimientos para manejar la seguridad de la tecnología de la información [4]. Estas acciones incluyen la identificación de las necesidades de la seguridad de la información, la puesta en práctica de las estrategias para satisfacer estas necesidades, medir los resultados, y mejorar las estrategias de protección.

Este entorno seguro debería considerar un conjunto de elementos que, de manera integrada, participarían en el sistema de gestión de seguridad de la información (ver Fig. 1). Los estándares pueden incluir aspectos técnicos, como seguridad en redes, firma digital, control de acceso, no repudio, gestión de claves, etc. Los procedimientos pueden ser operacionales, técnicos y de gestión. La auditoría, certificación y acreditación del sistema de gestión es importante para proporcionar credibilidad al entorno de seguridad. Evidentemente, un código de buenas prácticas, como la norma ISO/IEC 17799, es necesario para proporcionar los controles de seguridad a implantar y a gestionar. El sistema de gestión estará formado por un conjunto de procesos que dará lugar a un conjunto de productos. Éstos ayudarán a asegurar un nivel de seguridad adecuado, que dependerá de las necesidades particulares de seguridad. Todo este entorno tendrá en cuenta aspectos legales, sociales, éticos y culturales propios del entorno en el que se encuentre la empresa.

Uno de los aspectos más relevantes en la norma ISO/IEC 17799 ha sido su aportación para controlar los mecanismos de outsourcing de los servicios de los sistemas de información de las empresas [5], ya que este proceso de externalización está empezando a ser utilizado de forma masiva por todas las compañías para minimizar costes sin tener en cuenta que puede suponer nuevos riesgos en la seguridad, ya que normalmente se desconocen los niveles de seguridad que tienen las compañías con las que se externalizan los servicios.

Un conjunto de factores que consideramos críticos para el éxito de los SGSI son los siguientes:

- Enfocar la seguridad hacia el negocio.

- Implementar la seguridad en consonancia con la cultura de la empresa.
- Conseguir el apoyo indiscutible, visible y comprometido de la dirección de la empresa.
- Conseguir entender bien los requisitos de seguridad, evaluación y gestión de los riesgos.
- Concienciar tanto a directivos como a empleados de la necesidad de la seguridad.
- Ofrecer formación y guías sobre políticas y normas a toda la organización.
- Definir un sistema de medición para evaluar el rendimiento de la gestión de la seguridad y sugerir mejoras.

Fig. 1. Aspectos a cubrir en un SGSI (Eloff y Eloff, 2003)

3 Esquema de Implantación de Sistemas de Gestión de Seguridad

A pesar de la relevancia de la norma ISO/IEC 17799 tanto en el ámbito nacional como internacional, no podemos decir que proporcione un sistema de gestión de seguridad de la información, sino un conjunto de controles que nos sirven de guía para realizar una revisión detallada de la situación de nuestros sistemas en cuanto a seguridad. No obstante, y aunque no todos los controles que podemos encontrar en la norma son aplicables en todas las empresas, es recomendable que las organizaciones se preparen para esta norma, al menos como punto de partida [6]. Así, por ejemplo, la universidad de Pittsburgh está emprendiendo el desarrollo y la puesta en práctica de

un estándar comprensivo de la seguridad basado en las guías proporcionadas por el estándar de la seguridad de la ISO/IEC 17799 [7]. Aunque, como se indica en Eloff y Eloff (2003), se sugiere ir realizando una implantación progresiva de controles que permita que la empresa pueda irse adaptando a la evolución de la seguridad de una forma no traumática. Otros estudios consideran importante la norma, pero la complementan de alguna forma con otros aspectos, como es el caso de [8], que incorpora los requisitos de la HIPAA norteamericana a un programa de seguridad complementando la ISO/IEC 17799; [9], que considera una aplicación conjunta y complementaria de los COBIT y la norma; o incluso Masacci [10], que además de la norma considera controles relativos al cumplimiento de la legislación italiana en materia de protección de datos y privacidad. Otros, insisten en utilizar la 17799 en modelos de gestión de seguridad, pero siempre haciéndolo de manera incremental, considerando las necesidades particulares de seguridad [11].

Por lo tanto, aunque la norma no sea un sistema de gestión de la seguridad propiamente dicho, hay muchos autores que manifiestan su interés en desarrollar sistemas de gestión de la seguridad basados en ella.

La Gestión de la seguridad de la información puede ser implantada desde varias perspectivas: desde una perspectiva estratégica, afrontándolo mediante el gobierno corporativo y las políticas; o bien desde el punto de vista "humano", intentando implantar una cultura de la seguridad, formación, aspectos éticos, etc. [4].

Fig. 2. Modelo en espiral para madurez de los SGSI.

El modelo que más eficiente se ha mostrado para los clientes de SICAMAN ha sido el basado en la creación de ciclos de mejora mediante el modelo en espiral que podemos ver en la Fig.2. Este modelo facilita la realización de ciclos rápidos y

económicos que permiten crear una cultura de seguridad en la organización, de forma constante y progresiva.

Mediante este modelo, podemos estimar en un plazo mínimo de tiempo el nivel de madurez del SGSI de la empresa e identificar el reglamento que más se adapta ella, trazando hitos realistas a corto plazo de la evolución esperada en la empresa para cada ciclo de la espiral.

Este modelo está basado en tres niveles de protección, que aplicaremos según el nivel de madurez de la empresa y el tamaño de la misma. De esta forma, una empresa que según los parámetros de empleados y facturación se considere pequeña sólo debería aplicar la versión de la norma ISO17799-1 sobre 100 reglas de obligado cumplimiento (ver Fig.3). Cualquiera de las otras dos versiones de la norma (sobre 300 y 500 reglas) supondría sobredimensionar la seguridad de la empresa. Esto conllevaría un aumento del nivel de riesgo de que los controles implantados no sean sostenibles y produciría una degradación continua de los controles y del nivel de madurez.

Nivel de madurez (Según pre-auditoria realizada sobre la norma ISO17799)		**Tipo de Empresa (según nº de empleados y facturación)**		
Valoración Seguridad	**Nivel de madurez**	**Pequeña**	**Mediana**	**Grande**
		0 – 25 Empleados	25 – 250 Empleados	>250 Empleados
		0 – 1 Millones €	1 – 100 Millones €	>100 Millones €
0 - 30%	Bajo	ISO17799-1 (100)	ISO17799-1 (100)	ISO17799-1 (100)
30% - 70%	Medio	ISO17799-1 (100)	ISO17799-2 (300)	ISO17799-2 (300)
70 - 100%	Alto	ISO17799-1 (100)	ISO17799-2 (300)	ISO17799-3 (500)

Fig. 3. Modelos propuestos según el tipo de empresa y su nivel de madurez.

Una de las principales y más valiosas conclusiones obtenidas de la realimentación de los clientes de SICAMAN en los que se han analizado estos modelos es la siguiente: el sobredimensionamiento del nivel de seguridad de una empresa con respecto a su tamaño termina produciendo una degradación de los controles sobredimensionados, hasta que estos alcanzan su equilibrio natural. La consecuencia final de esto es que la empresa invierte un mayor número de recursos de los estrictamente necesarios, que no aportarán valor alguno. En la Fig.4, podemos ver una simulación de cómo, según el tamaño de la empresa, existe una tendencia natural de los sistemas de seguridad a encontrar su equilibrio.

Otros modelos que actualmente estamos desarrollando incluyen nuevos factores que pueden afectar a la hora de decidir sobre el nivel de cumplimiento que se debe aplicar: el tipo de actividad de la empresa, la dependencia de departamentos (como el de I+D), etc.

Eloff y Eloff [4] se decanta por definir cuatros clases distintas de protección, que permiten ir incrementando de forma progresiva los niveles de seguridad, en lugar de los tres seleccionados por nosotros.

- Clase 1: Protección inadecuada. No cubre ninguna sección de la ISO17799.

- Clase 2: Protección mínima. Cubre aspectos legales y de continuidad del negocio.
- Clase 3: Protección razonable. A los anteriores se le suman aspectos organizativos, control de activos y gestión de accesos.
- Clase 4: Protección adecuada: Cubre todas las secciones de la ISO17799.

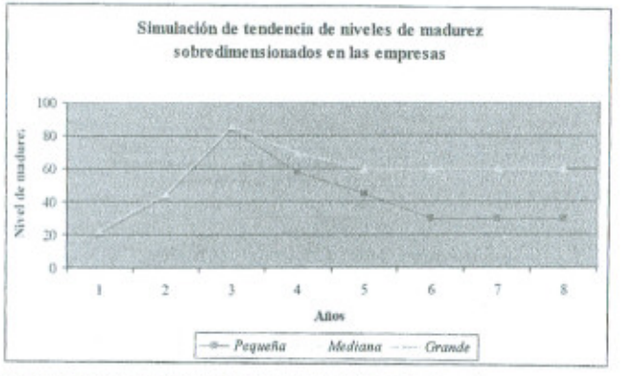


Fig. 4. Simulación de tendencia de niveles de madurez sobredimensionados en las empresas.

Una representación del modelo que propone lo podemos ver en la Fig.5. En gris, vemos las secciones de la norma que no se cumplen para ese nivel de protección.

ISO17799 Nombre de sección	**Clases de protección**			
	Clase 1: Protección inadecuada	**Clase 2: Protección mínima**	**Clase 3: Protección razonable**	**Clase 4: Protección adecuada**
Política de Seguridad				
Organización de la Seguridad				
Clasificación y Control de activos				
Política de personal				
Seguridad física				
Comunicaciones y operaciones				
Control de acceso				
Desarrollo y mantenimiento de sistemas de información				
Continuidad del negocio				
Satisfacción del marco legal y contractual				

Fig. 5. Ejemplo de asociación entre las secciones de la ISO17799 y las clases de protección.

Nuestro modelo, por el contrario, no asocia niveles de protección con secciones de la norma, sino que divide cada sección en tres niveles y sobre esos niveles podemos evolucionar la norma.

Aún cuando el método que proponemos permite evolucionar la protección a nivel de sección, no es aconsejable aplicarlo de esa forma. Lo ideal sería que el plan de mejora propuesto se adapte a la unificación de las diferentes secciones antes de acometer un segundo nivel de evolución de la norma, si éste fuera necesario.

En la Fig.6 podemos ver un modelo de madurez representado mediante nuestro "modelo de espiral". Aún cuando las diferentes secciones podrían avanzar de forma independiente, lo lógico es que planifiquemos mejorar aquellos aspectos que tienen una menor seguridad. En el caso del ejemplo, deberíamos mejorar la sección de "control de acceso" antes que cualquier otra sección.

Fig. 6. Ejemplo de niveles de madurez por secciones en el modelo de espiral.

Una vez establecidos los niveles de protección que deseamos utilizar, nos hemos planteado llevar a cabo un enfoque sistemático para abordar la implantación de sistemas de gestión de la seguridad de la información. Se ha considerado como núcleo principal la 17799, pero sin renunciar a otro tipo de estándares y recomendaciones en materia de seguridad y de gestión de seguridad. Los procesos principales se pueden ver en la Fig. 7.

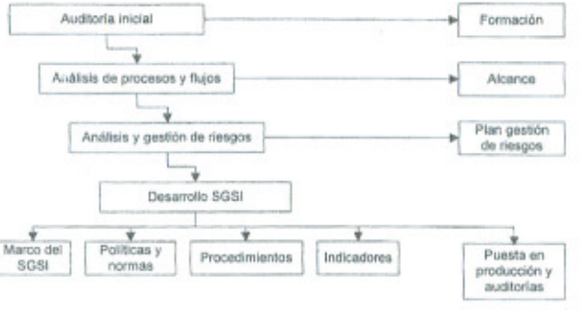


Fig. 7. Fases en la implantación de un SGSI

Una breve descripción de estas etapas es la siguiente:

- Auditoría Inicial. En un SGSI lo primero que debemos hacer es conocer la situación actual de la empresa con respecto a la seguridad y conocer a la empresa como organización. Esta fase implica establecer el nivel de madurez actual del SGSI en la empresa. Para ello, utilizamos un conjunto de checklist basados en la norma ISO17799 que son entregados a personas claves de la organización. El resultado de estos checklist se procesa para determinar inconsistencias y establecer, de una forma rápida y económica, una primera aproximación al nivel de madurez actual de la empresa. Esto nos permitirá decidir la versión de la norma ISO17799 que deseamos implantar, según nuestro modelo (ver Fig.5).
- Análisis de procesos y flujos. A partir del análisis previo del nivel de seguridad podremos llegar a realizar un análisis de los procesos y flujos necesarios para alcanzar el objetivo. Los entregables de esta fase incluyen los estándares específicos basados en los conceptos de la disponibilidad, de la integridad, y del secreto de la información. Al finalizar esta fase, conoceremos el estado actual y hasta qué nivel deseamos llevar la seguridad de la empresa (ver Fig. 8).
- Análisis y Gestión del Riesgo. Es una de las fases más importantes y sobre la que más estudios se están realizando. A pesar de ello, un enfoque basado en análisis y gestión de riesgos no es suficiente [12] sino que, además de identificar y eliminar riesgos, también esta actividad se ha de realizar de manera eficiente, ahorrando dinero, consecuencia directa de una correcta gestión de la seguridad [13]. Gracias al análisis de riesgos podremos identificar los activos y conocer el nivel de seguridad que debemos aplicarles. En la nueva norma ISO17799:2005 el análisis de riesgos se ha convertido en uno de los ejes principales, y la tendencia actual es convertirlo en una parte fundamental para un análisis y mantenimiento objetivo de la seguridad de una empresa.

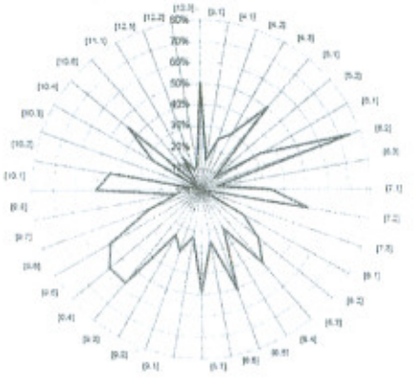


Fig. 8. Diagrama de kiviat del nivel de seguridad de la empresa por objetivos de control.

- Desarrollo del SGSI: Una vez conocida la situación actual real en cuanto a seguridad de la información, se elabora el sistema de gestión de seguridad de la información, definiendo un conjunto de controles de seguridad obtenidos de la norma ISO/IEC 17799 y teniendo en cuenta las particularidades de la empresa y los sistemas (que vendrán descritas en el marco o entorno del SGSI y en las políticas de la empresa). Además, se definirán unos procesos de gestión que consideren la revisión, control y mejora de los elementos de seguridad identificados, y que se basarán en un conjunto de indicadores de seguridad que muestren una visión cuantitativa de los controles de seguridad. Finalmente, se decidirá un plan de producción y puesta en marcha para el sistema de gestión de seguridad.

Adicionalmente, una de las tendencias de mercado durante la implantación de los SGSI es el desarrollo de un SCOREBOARD (Cuadro de mandos) que permita a la dirección tener un conocimiento inmediato de fallos y mejoras que se producen en sus sistemas. Para dicho fin, hemos desarrollado un prototipo orientado a asociar las secciones, objetivos de control y controles de la ISO/IEC 17779 a un scoreboard que mediante un código de colores indique a la dirección de la empresa qué aspectos de seguridad debe mejorar. Una pequeña muestra de este prototipo se puede ver en la Fig. 9, en la que se muestra el cuadro de mando a nivel de sección, y en la Fig. 10, en la que se muestra a nivel de objetivo de control. También se puede mostrar a nivel de control de seguridad individual.

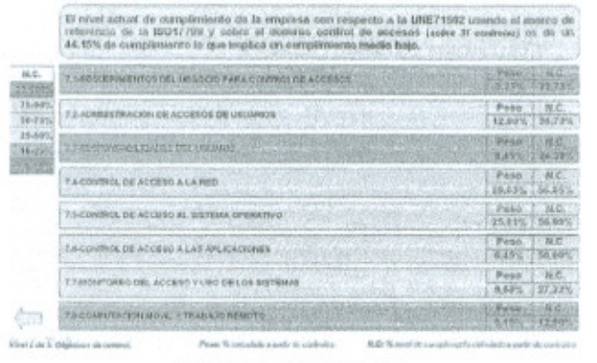


Fig. 9. Scoreboard a nivel de sección

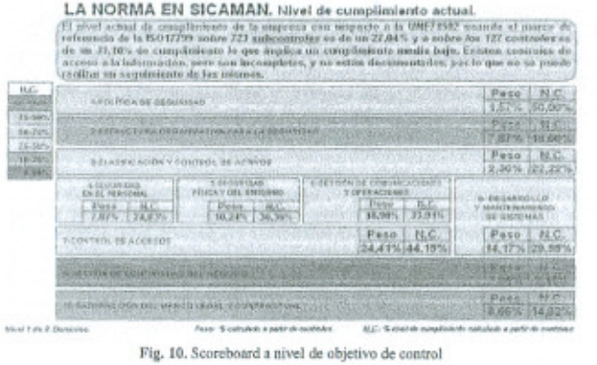


Fig. 10. Scoreboard a nivel de objetivo de control

La idea de este prototipo es poder integrar toda la información de las diferentes herramientas de seguridad existentes en las empresas en una sola herramienta que, mediante el desarrollo de métricas de seguridad, permita poder actualizar (con el mínimo de interacción humana) el cuadro de mando propuesto en las Figuras 9 y 10. Esto posibilitara que las empresas puedan conocer en todo momento el estado de su seguridad, invirtiendo para ello el menor número de recursos posibles. Para conseguir esto, nuestro prototipo se enfrenta al reto de tomar decisiones basadas en las incidencias comunicadas por el personal, alertas detectadas, etc.

4 Conclusiones y Trabajo Futuro

A pesar de los enormes esfuerzos que se están realizando para crear normativas de seguridad y métricas adecuadas para gestionar la seguridad en las empresas, éstas no terminan de encajar con el entorno en que deben ser implantadas. La causa más probable es la falta de madurez de las empresas y el haber intentado realizar normativas demasiado generales. Esto hace que muchas veces las empresas no sepan cuál es el alcance que deben cumplir, o por donde deben empezar a acometer la reestructuración de sus sistemas. Uno de los documentos generados por grupos internacionales de estandarización que mayor proyección ha tenido en el ámbito internacional es el código de buenas prácticas ISO/IEC 17799, que define un conjunto muy amplio de controles de seguridad. No obstante, este código de buenas prácticas no ofrece una solución global al problema de la seguridad porque carece de mecanismos de gestión.

En este artículo nosotros presentamos, desde nuestra experiencia práctica, una primera aproximación a la implantación de sistemas de gestión de la seguridad en pequeñas y medianas empresas, tomando como base o marco de referencia la norma tan mencionada en este artículo, y adaptándola para ajustarla al tamaño de la empresa en que se desee implantar y a su nivel de madurez.

Puesto que esta propuesta es muy preliminar, nuestro objetivo a medio y largo plazo es investigar en el desarrollo completo de una metodología para implantar sistemas de gestión de seguridad que permita una adaptación adecuada, dependiendo de las necesidades de seguridad y de las características de las empresas, principalmente enfocado a las pequeñas y medianas empresas. Esta metodología estaría basada en los principales estándares de seguridad y de gestión de seguridad, y se adaptaría a las condiciones sociales y, sobre todo, legales del entorno en el que desarrollamos nuestra actividad profesional. Mediante el método de investigación "en acción", con la ayuda de la retroalimentación obtenida directamente de nuestros clientes, esperamos conseguir una mejora continua de estas implantaciones.

Esta metodología se verá complementada con una herramienta de gestión de sistemas de seguridad, orientada principalmente a la gerencia, para facilitar la toma de decisiones a la hora de realizar las planificaciones de los sistemas de seguridad.

Agradecimientos

Esta investigación es parte de los proyectos DIMENSIONS, parcialmente financiado por el FEDER y por la Consejería de Educación y Ciencia de la Junta de Comunidades de Castilla-La Mancha (PBC-05-012-1), CALIPO (TIC2003-07804-C05-03) y RETISTIC (TIC2002-12487-E) concedidos por la "Dirección General de Investigación del Ministerio de Ciencia y Tecnología" (España).

Referencias

1. Dhillon, G. y Backhouse, J. Information System Security Management in the New Millennium. Communications of the ACM, (2000) 43(7).
2. Tsujii, S. Paradigm of Information Security as Interdisciplinary Comprehensive Science. Proc. of the 2004 International Conference on Cyberworlds (CW'04), IEEE Computer Society, (2004) 1-12.
3. Computer Security Institute – CSI. Computer Crime and Security Survey. (2002)
4. Eloff, J. y Eloff, M. Information Security Management – A New Paradigm. Proc. of the 2003 annual research conference of the South African institute of computer scientists and information technologists on Enablement through technology SAICSIT'03, (2003) 130-136.
5. Power, E.M. y Trope, R.L. Adverting Security Missteps in Outsourcing. IEEE Security & Privacy, marzo/abril, (2005) 70-73.
6. Peltier, T.R. Preparing for ISO 17799. Security Management Practices, jan/feb, (2003) 21-28.
7. Walton, J.P. Developing an Enterprise Information Security Policy. Proc. of the 30th annual ACM SIGUCCS conference on User services, (2002) 153-156.
8. Endorf, C. Outsourcing Security: The Nedd, the Risks, the Providers, and the Process. Information Security Management, (2004) 17-23.
9. Von Solms, B. Information Security governance: COBIT or ISO 17799 or both? Computers & Security 24, (2005) 99-104.
10. Masucci, P., Prest, M., Zannone, N. Using a security requirements engineering methodology in practice: The compliance with the Italian data protection legislation. Computer Standards & Interfaces 27, (2005) 445-455.
11. Von Solms, B. y Von Solms, R. Incremental Information Security Certification. Computers & Security 20, (2001) 308-310.
12. Siegel, C.A., Sagalow, T.R. y Serritella, P. Cyber-Risk Management: Technical and Insurance Controls for Enterprise-Level Security. Security Management Practices, sept/oct, (2002) 33- 49.
13. Garigue, R. y Stefaniu, M. Information Security Governance Reporting. Information Systems Security, sept/oct, (2003) 36-40.