CIASI 2001

III Congreso Iberoamericano de Auditoría y Control de Sistemas de Información

Madrid, 12-14 de Diciembre de 2001

Libro de Actas

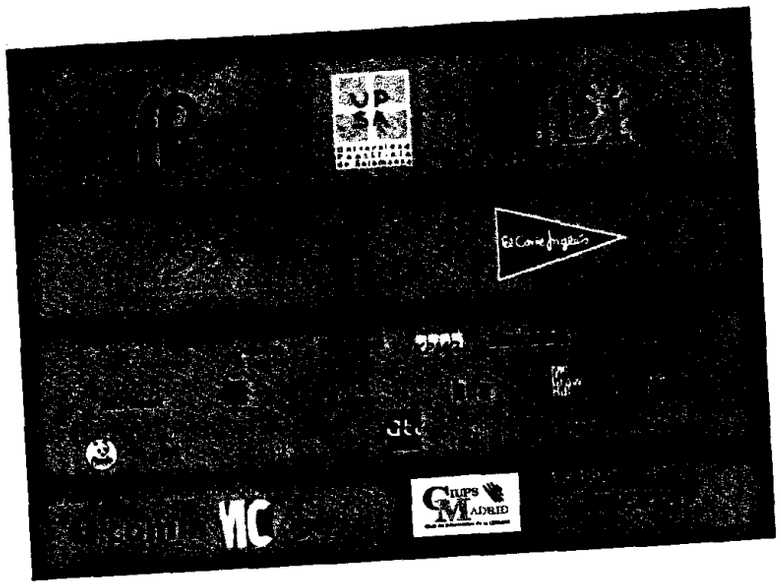
UNIVERSIDAD PONTIFICIA DE SALAMANCA EN MADRID
FUNDACIÓN PABLO VI

UNIVERSIDAD PONTIFICIA DE SALAMANCA
(*Campus Madrid*)

CIASI 2001
III Congreso Iberoamericano de Auditoría y Control de Sistemas de Información

LIBRO DE ACTAS

Madrid 12, 13 y 14 de Diciembre del 2001



Editores:
Carlos Manuel Fernández Sánchez (UPSAM / BSA),
Luis Joyanes Aguilar (UPSAM), Mario Piattini Velthuis (UCLM),
Marina Touriño Touriño (CISA-ISACA)

ISBN : 84-669-6795-9

Depósito legal: M-52692-2001

Imprime: Gráficas Arias Montano, S.A.
28935 MÓSTOLES (Madrid)

COMITÉ DE HONOR

D. Julio Manzanares Marijuan.
Excmo. y Magnifico Sr. Rector de la Universidad Pontificia de Salamanca
D. José María Guix.
Excmo. Sr. Presidente de la Fundación Pablo VI
D. José María Alvarez del Manzano.
Excmo. Sr. Alcalde de Madrid
D. Isidoro Alvarez
Excmo. Sr. Presidente de El Corte Inglés y de la Fundación Ramón Areces
D. Gustavo Villapalos Salas.
Excmo. Sr. Ex-Consejero de Educación Comunidad de Madrid
D. Fernando González-Moya Rodríguez de Mondelo.
Excmo. Sr. Presidente del Consejo General de Colegio de Economistas
D. Juan Jiménez Aguilar.
Excmo. Sr. Secretario General de la CEOE
D. Angel Berna Quintana.
Ilmo. Sr. Director de la Fundación Pablo VI
D. Manuel Capelo Martínez.
Ilmo. Sr. Decano de la Facultad de Informática de la Universidad Pontificia de Salamanca en Madrid
D. Francisco Roman.
Ilmo. Sr. Director General de Microsoft, Ibérica

COMITÉ DE PROGRAMA

Presidentes
D. Carlos Manuel Fernández Sánchez (UPSAM / BSA)
D. Luis Joyanes Agular (UPSAM)
D. Mario Piattini Velthuis (UCLM)
D. Marina Touriño Touriño (CISA-ISACA)

Miembros
D. Vidal Alonso Secares (UPSA)
D. Miguel A. Amutio Gómez (MAP)
D. Ramiro Cárdenas (UTPL, Ecuador)
D. Juan M. Cueva Lovelle (U. Oviedo)
D. Miguel Angel Davara Rodríguez (ULPGC)
D. Jose Antonio Echenique Garcia (UNAM, México)
D. Manuel García García (BS)
D. Victor Martin García (UPSAM)
Dña. Mª José Gil Larrea (UD)
D. Manuel González (ULPGC)
D. Juan Carlos Granja (UG)
D. Antonio Guardiola Lozano (UPSAM)

D. Antonio Guevara Plaza (UMA)
D. Alonso Hernández García (OAI)
D. Josep Jover (Studios Juridic)
D. Aquilino Adolfo Juan Fuente (Colegio Ingenieros Informáticos de Asturias)
D. David La Red Martínez (UNNE, Argentina)
Dña. Paloma Llaneza González (LlyA)
Dña. Luz Mayela Ramírez (UCC, Colombia)
D. Victor Hugo Medina García (UDFJC, Colombia)
D. Ramiro Merchán Patarroyo (CISA, UCC, Colombia)
D. Ramón Miñones Crespo (UCV)
D. Lucio A. Molina Focazzio (CISA, UAN, Colombia)
D. Jorge Páez Mañá (CINDOC, CSIC)
D. Eloy Peña Ramos (UMA)
D. José Nelson Pérez Castillo (UDFJC, Colombia)
D. Emilio del Peso Navarro (IEE)
D. José Ramón Pin (IESE)
Dña. Isabel Ramos (US)
D. Miguel A. Ramos (IEE, UC3M)
D. Arturo Ribagorda (UC3M)
D. Jesús Ribero Laguna (Fundación Dintel)
D. Javier Rivas (PWC)
D. José Antonio Rodero Rodero (UMU)
D. Luis Rodriguez Baena (UPSAM)
D. Gustavo Rossi (UTN, Argentina)
D. Manuel Ruíz de Aldereguía (Alderan - Grupo OHL)
D. Francisco Ruiz González (UCLM)
D. Joaquín Sánchez Villoria. (Altadis / UPSA)
D. Gustavo A. Solís Montes (CISA, GRUPO CYNTHUS, México)
D. Emilio Suñer (UCM)
D. José Luis Tejeda (AENOR)
D. Johann Tello Meryk (CISA, ISACA, Panamá)
D. Jorge Torres (ISEM/TEC, México)
D. Virgilio Yague Galaup. (BBVA / UPSAM)
D. Patricio Yustas Torijano (Getronics / UPSAM)

LEYENDA

UPSA	Universidad Pontifica de Salamanca
UPSAM	Universidad Pontifica de Salamanca campus Madrid
MAP	Ministerio de Administración Pública
UTPL	Universidad Técnica Particular de Loja, Ecuador
U.Oviedo	Universidad de Oviedo
ULPGC	Universidad de las Palmas de Gran Canaria
UNAM	Universidad Nacional Atónoma, México
BS	Banco de Sabadell
UD	Universidad de Deusto
UG	Universidad Granada
UMA	Universidad de Málaga
OAI	Organización de Auditoría Informática
UNNE	Universidad Nacional del Nordeste, Corrientes Argentina
LlyA	Llaneza y Abogados
UCC	Universidad Católica de Colombia
UDFJC	Universidad Distrital Francisco José de Calda, Colombia
CISA	Certificación de Auditoría de Sistemas de Información
UCV	Universidad de la Coruña Virtual
UAN	Universidad Antinio Nariño
CINDOC	Centro de Información y Documentación Científica
IEE	Informáticos Europeos Expertos
UC3M	Universidad Carlos III de Madrid
CSIC	Centro Superior de Investigaciones Científicas
IESE	Instituto de Estudios Superiores de la Empresa
US	Universidad de Sevilla
PWC	Price Waterhouse Coopers
UMU	Universidad de Murcia
UTN	Universidad Tecnológica Nacional Argentina
OHL	Obrasión, Huarte y Lain
UCLM	Universidad de Castilla – La Mancha
UCM	Universidad Complutense de Madrid
AENOR	Asociación Española de Normalización y Certificación
ISACA	Asociación de Auditoría y Control de Sistemas de Información
ITESM	Instituto Tecnológico y de Estudios Superior de Monterrey, México.
BBVA	Banco Bilbao Vizcaya Argentaria

COMITÉ DE ORGANIZACIÓN

Presidente del Congreso
D. Luis Joyanes Aguilar

Miembros
Dña. Marina Touriño Touriño, Coordinadora CISA-ISACA
D. Carlos Fernández Sánchez, UPSAM
D. Victor Martín García, UPSAM
D. Juan Manuel Lombardo Enríquez, UPSAM
D. Javier Parra Fuente, UPSAM
D. Enrique Torres Franco, UPSAM
D. Angel González del Alba Baraja, UPSAM
Dña. Sara Gallego Trijueque, UPSAM
Dña. María P. Dorrego de Luxán, UPSAM
D. Daniel García Sánchez, UPSAM
D. Rafael Fuertes, FPVI
D. Alfonso López Rivero, UPSA
D. Alonso Hernández García, OAI
D. Ramón Miñares Crespo, OAI
D. Clemente Martín, UPSAM
D. Sergio Rios Aguilar, UPSA
Dña. Juana González González, UPSAM
D. Ángel Paredes Icaza, PUCP, Perú
Dña. Paloma Centenera Centenera, UPSAM
Dña. Maria Luisa Díez Platas, UPSAM

SECRETARIA TÉCNICA

Jefe de Secretaría Técnica
D. Victor Martín García, UPSAM
Responsable de Secretaría Técnica de Organización
D. Juan Manuel Lombardo Enriquez, UPSAM
Responsable de Secretaría Técnica de Programa
Dña. Mar Escribano Castellanos, UPSAM
Relaciónes Institucionales de Auditoría
Dña. Marina Touriño Touriño
Relaciónes con Empresas
D. Daniel García Sánchez, UPSAM
Relaciónes Académicas
D. Angel González del Alba, UPSAM
Responsables de Relaciónes con Medios de Comunicación
D. Miguel Ballesteros Martínez, UPSAM
Dña. Victoria Joyanes Delgado Ureña, UPSAM
Responsable de Relaciónes Institucionales
Dña. Maria Luisa Díez Platas, UPSAM

Responsable de Ingeniería Web
D. Javier Parra Fuente, UPSAM
D. Oscar Sanjuan Martínez, UPSAM

Colaboración Especial

Club de Informáitca de la Universidad Pontificia de Salamanca en Madrid (CIUPS)

Manuel Durán Oñate

Javier Pascual Soriano

Delegación de Alumnos de Informática de la Universidad Pontificia de Salamanca en Madrid

Delegación de la Facultad de Informática

Delegación de la Escuela Universidad de Informática

PROGRAMA

Miércoles, 12 de Diciembre de 2001

AUDITORÍA INFORMÁTICA

8:00 Acreditación y recogida de documentación

9:00 Inauguración y Discurso de apertura

D. JULIO MANZANARES MARIJUAN
Excmo y Magnífico Sr. Rector de la Universidad Pontificia de Salamanca
D. JUAN MANUEL FERNÁNDEZ LÓPEZ
Director de la Agencia de Protección de Datos
D. LUIS JOYANES AGUILAR
Presidente de CIASI 2001

Primera Sesión: Auditoría de Sistemas de Información

9:30 1ª Conferencia Plenaria: *Gestión y Auditoría de los Sistemas de Información y Estrategias de Futuro.*
D. GUSTAVO ADOLFO SOLIS MONTES
Presidente del Grupo Cynthus (México)
CISA- Ex Vicepresidente de ISACA para *Latinoamérica*
Autor del Libro *"Reingeniería en Auditoría en Informática"*

10:30 2ª Conferencia Plenaria: *Retos para la Auditoría de Sistemas y Tecnología de la Información frente a los cambios tecnológicos*
D. PABLO LANZA
Auditor de Sistemas de Información en la Administración Pública - CISA
Dª. SUSANA MENDIOLA-OLAECHEA
Responsable de Auditoría de Sistemas de Información.
Banco Guipuzcoano- CISA

11:30 Descanso

12:00 Mesa Redonda: *Situación y Estrategias de la Auditoría de Sistemas de Información en España y Latinoamérica.*
Moderador: Dª MARINA TOURIÑO TOURIÑO
Coordinadora CISA España- ISACA
D. JESUS MERINO
Socio de Auditoría Informática. (Ernst & Young).
D. DIEGO RODRÍGUEZ
Auditoría Informática. (Deloitte & Touch)

D. JUAN MIGUEL RAMOS
Socio de Auditoría Informática. (Andersen)
Dª PALOMA HERNÁNDEZ
Senior Manager de KPMG_IRM

14:00 Final de sesión de mañana

TARDE

Sesión T1.1. (Paralela)

16:00 Presentación de Comunicaciones

17:15 *Protección de Antivirus y su Auditoría*
Dª. M. VICTORIA RETRESPO
Panda Software

17:45 *Seguridad .NET*
Dª. IDOIA MATEO
Responsable .NET
Andersen

18:15 Conferencia Plenaria Tarde: *Security Concerns On Wireless Networks*
D. DAVID BRADSHOW
Director de Tecnologías Inalámbricas
Intel Corporation Europa

Sesión T1.2 (Paralela)

16:00 Presentación de Comunicaciones

17:15 *Certificación AENOR*
D. MIGUEL ANGEL MARTÍNEZ
Ejecutivo de AENOR

18:00 *Evaluación de Riesgos y Plan de Contingencia*
D. ANTONIO GUTIERREZ
Manager KPMG_IRM

18:15 *Conferencia Plenaria Tarde: Security Concerns On Wireless Networks*
D. DAVID BRADSHOW
Director de Tecnologías Inalámbricas
Intel Corporation Europa

Sesión T1.3 (Laboratorio)

16:00 Tutorial de COBIT: *Implantación basada en Sistemas de Aseguramiento de Calidad ISO 2000*
D. RAMIRO MERCHÁN
Universidad Católica de Colombia, Bogotá (Colombia) -CISA

19:00 a 20:30 Mesa Redonda: *Control, Auditoría y Medición de Audiencias en Sitios Web.*
Moderador: D. MIGUEL BALLESTEROS MARTÍNEZ
Profesor de Marketing y Logística (UPSA Madrid, Facultad de Informática)
D. ANTONIO ANGUITA
Director de EresMas
D. MIGUEL PÉREZ SUBÍAS
Presidente de la Asociación de Usuarios de Internet
D. NURIA LLEDÓ
Directora de Jupiter MMXi España
D. IGNACIO DEL VILLAR GARCÍA
DMR

Jueves, 13 de Diciembre de 2001

SEGURIDAD Y PROTECCION DE LA INFORMACION Y DEL CONOCIMIENTO

Segunda Sesión: Seguridad de Sistemas de Información

9:00 1ª Conferencia Plenaria: *Nuevas Tendencias en la Seguridad de los Sistemas y Tecnologías de la Información*
D. JOSE MAÑAS
Universidad Politécnica de Madrid. Consultor Independiente.
D. CARLOS JIMÉNEZ
Director General de Secuware

10:30 2ª Conferencia Plenaria: *Legislación de los Sistemas de Tecnologías de la Información y su Auditoría*
D. PALOMA LLANEZA
Llaneza Abogados

11:30 Descanso

12:00 Mesa Redonda: *Situación y Estrategias de la Auditoría de Sistemas de Información en España y Latinoamérica.*

MODERADOR: D. CARLOS MANUEL FERNÁNDEZ
Vicepresidente de Business Software Alliance /UPSA

D. ALEJANDRO ALIAGA
Asuntos legales. El Corte Inglés
D. XAVIER RIBAS
Abogado Especialista en Legislación Informática
Socio de Landwell PWC
D. MIGUEL ANGEL DAVARA RODRIGUEZ
Director del Instituto de Informática Jurídica
Universidad Pontificia Comillas
D. JOSEP JOVER
Representante de Estudios Jurídicos
D. JOSE MARIA ANGUIANO
Abogado Especialista en Nuevas Tecnologías
Socio de Garrigues & Andersen
D. IGNACIO JAVIER FERNÁNDEZ
Abogado Especialista en Nuevas Tecnologías
Socio de Ernst & Young
D. MONTIANO MONTIAGUDO
Bufete Uría Menéndez
Dª. CARMEN GUITERREZ DEL OLMO
Manager KPMG_IRM

14:00 Final de sesión de mañana

TARDE
Sesión T1.1. (Paralela)

16:00 Presentación de Comunicaciones

17:15 Firma Digital: *Proyecto CERES*
D. SERGIO RAMÓN RUIZ MAHÍLLO
Director del Proyecto CERES

18:00 Conferencia Plenaria Tarde: *Las Funciones de la Agencia de Protección de Datos*
D. JESÚS RUBÍ NAVARRETE
Adjunto Director de la Agencia de Protección de Datos

18:30 *Protección de Sistemas y Redes frente a actividades ilegales. Ciberdelincuentes.*
D. BERNARDINO CORTIJO
Director General de Seguridad Cooperativa Terra Network

Sesión T1.2 (Paralela)

16:00 Presentación de Comunicaciones

17:15 *Auditoría de una plataforma Wireless*
D. TEODORO LÓPEZ PALACIOS
Gerente DMR Consulting

18:00 Conferencia Plenaria Tarde: *Las Funciones de la Agencia de Protección de Datos*
D. JESÚS RUBÍ NAVARRETE
Adjunto Director de la Agencia de Protección de Datos

18:30 *Web Trust. SYS Trust, generando confianza en la Red*
Dª. MYRIAM OLONDO SERRANO
Senior Management Ernst & Young (TSRS)

19:00 a 20:30 Mesa Redonda: *Técnicas de Seguridad y Auditoría en Internet*
Moderador: D. FERNANDO DAVARA RODRÍGUEZ
Director del Centro Europeo de Satélites /UPSAM
D. GUSTAVO ADOLFO SOLIS MONTES
Presidente del Grupo Cynthus (México)
D. RAMIRO MERCHAN
Universidad Católica de Colombia, Bogotá (Colombia)
D. JOSE ANTONIO ECHENIQUE
UNAM, D.F. México
D. BERNARDINO CORTIJO
Director General de Seguridad Corporativa Terra Network
D. MANUEL LEA
Profesor de Sistemas Operativos, Facultad de Informática / UPSAM

Viernes, 14 de Diciembre de 2001

NORMAS DE VERIFICACION

Tercera Sesión: Certificación, Calidad y Normas de Verificación

9:00 1ª Conferencia Plenaria: *Auditoría y Control de Servidores de Aplicación en Web*

D. PETER ZADROZNY

EMEA, Techologist Chief

BEA Systems

Co-Autor del Libro Professional Java 2 Enterprise Edition With BEA WebLogic Server

10:30 2ª Conferencia Plenaria: *Metodologías de Auditoría de Sistemas de Información*

D. JOSE ANTONIO ECHENIQUE

UNAM, DF México (México)

11:00 3ª Conferencia Plenaria: *Seguridad y Auditoría de ERP´s*

D. RAMIRO MERCHAN

Profesor encargado de Auditoría Informática

Universidad Católica de Colombia, Bogotá (Colombia)

11:30 Descanso

12:00 Mesa Redonda: *Calidad y Certificación en Software-Normativas ISO/AENOR.*

MODERADOR: **D. MARIO PIATTINI**

Universidad Castilla La Mancha- CISA

D. ROBERTO MOYA

Coordinador del SubComité de Normas de Seguridad TI - CISA

AENOR – Certificado de Gestión del Software

D. JOSE LUIS TEJERA

Director de Desarrollo Estrátegico. (ISO 17799)

D. MIGUEL ANGEL AMUTIO

Consejero Técnico de Normas Tecnológicas.

Ministerio de Administraciones Públicas -CISA

13:45 Ceremonia de Claúsura

14:00 Final de Ceremonia de Claúsura

PRESENTACIÓN DEL COMITÉ DE ORGANIZACIÓN

Me cabe el honor en nombre del Comité de Organización y del Comité de Programa de este III Congreso Iberoamericano de Auditoría y Control de Sistemas de Información, de dirigirme a Vs. para presentarles CIASI 2001. Honor que agradezco en nombre de la Universidad Pontificia de Salamanca y de la Fundación Pablo VI que acogen y organizan este Congreso.

Hace 50 años las necesidades de proceso de datos se realizaban manualmente; hoy, los ordenadores realizan la mayoría del procesamiento de datos requerido tanto para los sectores públicos y privados. Como resultado de ello, aparece la necesidad de mantener la integridad de los datos procesados por los ordenadores a medida que estos penetran en nuestras vidas. Muchas personas tienen miedo de que las crecientes y poderosas capacidades de procesamiento de datos no estén bien controladas. Tenemos preocupación sobre la privacidad de los datos que intercambiamos con las organizaciones tales como los departamentos de hacienda , autoridades médicas o instituciones financieras. Quien de nosotros no ha sufrido las frustraciones de intentar que una organización actualice nuestros datos personales o profesionales y se ha enfrentado con "la burocracia de la informática".

El uso incontrolado de los ordenadores es sabido que puede tener una influencia negativa en la sociedad. Por ejemplo, la información errónea, imprecisa , producirá controles inadecuados de los sistemas de información que día a día controlan volúmenes de datos cada vez más difícil de procesar, reunir, medir y auditar. A medida que crece la sensación de "ubniquidad" de los ordenadores , muchas personas tienen un sentido de la perdida de la individualidad de su privacidad. " *El gran hermano"* de George Orwell de *1984* parece que vive con nosotros.

Necesidad del control y auditoría de los ordenadores

Los ordenadores se utilizan ampliamente para procesar datos, proporcionar información y convertirla en conocimiento para la toma de decisiones. La creciente potencia de los PC (procesadores de 1.5 GHz a 2 GHz., memorias de 256 K, discos duros de 40-60 Gigas, unidades de almacenamiento CD-RW y DVD, comienzan a ser características "casi" normalizadas en los PCs comerciales en los albores del año 2002), la implantación de la telefonía móvil 2G y 2.5G y la futura y deseada 3G (UMTS) que, probablemente, tendremos en el 2003, la revolución inalámbrica (con protocolos tales como . *Bluetooth,* LDMS,..) que anuncia la nueva sociedad *inalámbrica,* la creciente demanda de líneas telefónicas ADSL (más de 400.000 líneas implantadas en España a finales de Noviembre de 2001),... conducen a unas cifras de penetración de ordenadores y teléfonos inteligentes (PDAs con integración de teléfono) la Red Internet impensables hace tan solo un par de años.

Debido a este inmenso rol que juegan y van a jugar los ordenadores en el proceso de datos y en la toma de decisiones, es muy importante que su uso esté bien controlado. Ron Wiber. El gran *gurú* de la auditoría de sistemas de información en su prestigiosa obra.... señala siete importantes razones para que las organizaciones diseñen , estructuren y pongan en funcionamiento departamentos de control y

auditoría de sistemas de información o sistemas informáticos o de computación. Estos siete factores que deben influir en una organización para controlar y auditor los ordenadores son las siguientes:

1. Costes de la organización por pérdidas de datos
2. Costes por la toma de decisiones incorrectas
3. Costes en el abuso de los ordenadores
4. Valor del hardware, software y del capital humano
5. Altísimos costes de los errores informáticos
6. Mantenimiento de la privacidad
7. Evolución controlada del uso de los ordenadores.

Estos factores y algunos más que saldrán a lo largo de este congreso iberoamericano conducen de modo inequívoco a la necesidad de que una organización debe controlar y auditar los sistemas informáticos ya que los costes de los errores e irregularidades que se producen en los sistemas pueden ser muy altos, escandalosamente tan altos que no puedan ser soportados por las propias organizaciones. La capacidad de una organización para afrontar situaciones de riesgo, corrupciones y destrucciones de sus bases de datos, errores en la toma de decisiones producidas por sistemas de información de pobre calidad, pérdidas incurridas por el abuso informática, pérdidas de hardware y software valioso o lo que es peor capital humano; los altísimos costes de algunos tipos de errores informáticos, fallos en el mantenimiento de la privacidad de las personas individuales y fallos en el control de como los ordenadores han de utilizar correcta y fiablemente en las organizaciones.

Las funciones de la auditoría de sistemas de información han sido establecidas para salvaguardar activos, mantener integridad de los datos, conseguir unos sistemas eficaces y eficientes.

Muchos de los principios que fundamentan la práctica de los sistemas de auditoría de información tienen sus raíces en otras disciplinas tales como la auditoría tradicional (buena prueba de ello es la presencia de las cinco grandes en este salón), ciencia informática y de computación, economía y administración y organización de empresa, así como gestión (*management)* y recursos humanos, junto con las nuevas teorías, principios y los nuevos departamentos de Gestión del Conocimiento, que requerirán unirse a los actuales departamentos de auditoría de sistemas de información en la necesaria auditoría del conocimiento existente y futuro de las organizaciones.

Definición de Auditoría de Sistemas de Información

Muchas son las definiciones, como ocurre con cualquier término reconocido, de *auditoría de sistemas de información* o *auditoría informática*, como a veces se le conoce en la jerga de los departamentos de sistemas de información. En nuestro caso hemos elegido la definición dada por el citado Ron Weber en su obra más conocida: *"La auditoría de sistemas de información es el proceso de recolección (recogida) y evaluación de evidencia para determinar si un sistema informática salvaguarda*

activos, mantiene integridad de los datos, permite que los objetivos de la organización se consigan eficazmente y utiliza los recursos eficientemente". Por consiguiente, la auditoría de los sistemas de información soporta objetivos de la auditoría tradicional: legalizar objetivos (aquellos del auditor externo) que se centra en la salvaguardia de activos e integridad de datos, y gestión de objetivos (aquellos del auditor interno) que abarcan no solo la legalización de los objetivos sino también la eficacia y eficiencia de los mismos.

Los impactos de la Tecnologías de la Información en los Auditores

A medida que las **TIC** (Tecnologías de la Información y la Comunicación) y los modelos de negocios evolucionan irá variando el rol de los auditores. Los nuevos modelos de negocios basados en *outsourcing,* teletrabajo, redes tradicionales, virtuales e inalámbricas, gestión del conocimiento y gestión de competencias, .. así como las nuevas aplicaciones centradas en **ERP, EAI, CRM, EAI, SCM**, *e-procurement*, etc. requieren que el auditor se anticipe a la dirección estratégica de las TI y proporcionen planes y directrices para los procesos de negocio que permitan tomar decisiones acertadas y correctas.

Cada día un auditor se enfrenta a retos más críticos en términos de actualización en el conocimiento de las tecnologías más innovadoras y las tradicionales para propocionar la evaluación o valoración que requieren las nuevas tecnologías.

El rol del auditor en sistemas de información es clave en el gobierno de las TI que debe ir en paralelo con los objetivos del negocio y las necesidades de las organizaciones.

¿Qué debemos hacer en las universidades? La respuesta es sencilla: (1) Incorporar la disciplina de Auditoría de Sistemas de Información en los planes de estudio de pregrado : ingenierías técnicas y superiores; (2) Impartir la disciplina en cursos de postgrado e incluso cursos específicos de Auditoría de Sistemas de Información; (3) Investigación en la disciplina en colaboración con las empresas de auditoría y organizaciones profesionales. Nuestra universidad , pionera en los estudios de Auditoría Informática, introdujo esta asignatura en el año 1999 en los planes de estudio propios de Diplomado en Informática Fundamental y luego con la creación de nuestra Escuela universitaria y Facultad de Informática, en el año 1990, todos los planes de estudios de ingeniería técnica y superior han incluido una asignatura de Auditoría Informática, en 3° curso en un caso y en 5° curso en el otro. Respecto a la investigación , nuestra Facultad tiene un equipo de investigación en auditoría de sistemas de información dirigida por los profesores de la asignatura que está patrocinada, entre otras, por la BSA y que ya ha publicado varios artículos y presentado comunicaciones a congresos nacionales e internacionales, y prepara los trabajos de investigación necesarios para inscribir dos tesis doctorales.

Por último señalar como tema destacado e importante del congreso dos actos académicos paralelos que esperamos sean de gran relevancia para el futuro de la auditoría informática: el I Encuentro Iberoamericano de CISAs y la I Escuela

Internacional de Otoño de Sistemas de Información con un enfoque dirigido este año a la Auditoría de Sistemas de Información.

En la era de la información y el conocimiento en que vivimos el binomio *información-conocimiento* se ha convertido en el activo más importante de las organizaciones. Por otra parte, entendemos que "no hay conocimiento sin control interno de la información" . En consecuencia CIASI 2001 estudiará y analizará el estado actual de la auditoría de los sistemas de información y cómo la información-conocimiento pueden conducir a organizaciones más eficientes y eficaces.

En nombre del Comité de Organización confiamos que los objetivos que se fijaron por los diferentes comités se puedan cumplir y llevar a buen puerto.

Luis Joyanes Aguilar
Presidente de CIASI 2001

PRESENTACIÓN DEL COMITÉ DE PROGRAMA

Cuando en 1998 iniciamos las Jornadas sobre Auditoria Informática en la Universidad de Castilla La Mancha, nos dimos cuenta de la necesidad de un foro de encuentro y discusión para el intercambio de experiencias y conocimientos entre los principales profesionales e investigadores en el área del Control y la Auditoría de los Sistemas de Información. Dichas jornadas se consolidaron en el Congreso sobre Auditoría de Sistemas de Información, celebrado en Valencia y que constituyo un éxito tanto del punto de vista científico como de organización.

En esta tercera edición organizada por la Universidad Pontificia de Salamanca, el congreso se ha extendido a toda la comunidad iberoamericana, lo cual amplía considerablemente la temática a tratar y el conocimiento que podremos compartir.

Este volumen recoge los trabajos que han sido seleccionados de todos los enviados a este congreso, procedentes de más de diez países iberoamericanos. Además de las comunicaciones contamos con numerosos conferenciantes invitados: Gustavo Adolfo Solís expondrá el tema de la "Gestión y Auditoría de los Sistemas de Información y Estrategias de Futuro", Pablo Lanza y Susana Mendiola-Olaechea tratarán sobre los "Retos para la Auditoría de Sistemas y Tecnología de la Información frente a los cambios tecnológicos", José Mañas y Carlos Jiménez hablarán sobre las "Nuevas Tendencias en la Seguridad de los Sistemas y Tecnologías de la Información", Paloma Llaneza tratará sobre la "Legislación de los Sistemas y Tecnologías de la

Información y su auditoría", Peter Zardrozny comentará la "Auditoría y COntrol de Servidores de Aplicación en Web", José Antonio Echenique expondrá las "Metodologías de Auditoría de Sistemas de Información" y Ramiro Merchán tratará sobre la "Seguridad y Auditoría de ERP´s".

Esta edición ha apostado además por las mesas redondas. En efecto, se celebrarán varias durante el congreso: el primer día se debatirá la "Situación y Estrategias de la Auditoría de Sistemas de Información en España y Latinoamérica" y las "Técnicas de Seguridad y Auditoría de Internet", el segundo día se discutirá la "Experiencia de la LOPD y la Propiedad Intelectual del Software" y el "control, Auditoría y Medición de Audiencias en Sitios Web", y el último día se tratará sobre la "Calidad y Certificación en Software: Normativas ISO/AENOR".

Obviamente, este Congreso no hubiera sido posible sin la participación y colaboración de muchas personas. En primer lugar queríamos agradecer a ambas comunidades, profesional y científica, su apoyo enviando trabajos, propuestas de conferencias, mesas redondas, etc. Asimismo, nuestro más sincero reconocimiento a todos los miembros del Comité Organizador, por su entrega y dedicación durante que ha hecho posible la celebración de este congreso que esperamos resulte del interés de todos los que participan.

Mario Piattini (UCLM)
Carlos Fernandez (BSA)
Luis Joyanes (UPSA)
Marina Touriño (CISA/ISACA)

Madrid, Diciembre 2001

CONFERENCIAS PLENARIAS

Gestión y Auditoría de los Sistemas de Información y Estrategias de Futuro.
D. GUSTAVO ADOLFO SOLIS MONTES

Retos para la Auditoría de Sistemas y Tecnología de la Información frente a los cambios tecnológicos
D. PABLO LANZA
Dª. SUSANA MENDIOLA-OLAECHEA

Security Concerns On Wireless Networks
D. DAVID BRADSHOW

Nuevas Tendencias en la Seguridad de los Sistemas y Tecnologías de la Información
D. JOSE MAÑAS
D. CARLOS JIMÉNEZ

Legislación de los Sistemas de Tecnologías de la Información y su Auditoría
D. PALOMA LLANEZA

Las Funciones de la Agencia de Protección de Datos
D. JESÚS RUBÍ NAVARRETE

Auditoría y Control de Servidores de Aplicaciones en Web
D. PETER ZADROZNY

Metodologías de Auditoría de Sistemas de Información
D. JOSE ANTONIO ECHENIQUE

Seguridad y Auditoría de ERP´s
D. RAMIRO MERCHAN

CONFERENCIAS

Protección de Antivirus y su Auditoría
Dª. M. VICTORIA RETRESPO

Seguridad .NET
Dª. IDOIA MATEO

Certificación AENOR
D. MIGUEL ANGEL MARTÍNEZ

Evaluación de Riesgos y Plan de Contingencia
D. ANTONIO GUTIERREZ

Proyecto CERES
D. SERGIO RAMÓN RUIZ MAHÍLLO

Protección de Sistemas y Redes frente a actividades ilegales. Ciberdelincuentes.
D. BERNARDINO CORTIJO

Auditoría de una plataforma Wireless
D. TEODORO LÓPEZ PALACIOS
Gerente DMR Consulting

Web Trust. SYS Trust, generando confianza en la Red
Dª. MYRIAM OLONDO SERRANO

CONTENIDO

UML para el Diseño de Bases de Datos Seguras

Eduardo Fernández-Medina Patón
Universidad de Castilla-La Mancha. Departamento de Informática.
Ciudad Real, 13017. España.
efmedina@inf-cr.uclm.es

Mario Piattini Velthuis
Universidad de Castilla-La Mancha. Departamento de Informática.
Ciudad Real, 13017. España.
mpiattin@inf-cr.uclm.es

Abstract

In this article we argue the importance of security in databases, and the need to consider security as a fundamental requirement in their development and one which is integrated at all stages of design, instead of being an isolated and marginal requirement. We propose an extension of the Use Case and Class models of UML using their standard extension mechanisms (stereotypes, tagged values and constraints) to allow us to design multilevel databases. We carry out the necessary modifications on the meta-model of UML so that security level is considered as an intrinsic aspect of the elements of the models. Finally we show an example.

Keywords: *Secure databases, UML, security constraints, access control, multilevel databases, confidentiality, database design.*

RESUMEN

En este artículo se justifica la importancia de la seguridad en las bases de datos, y la necesidad de considerar la seguridad como un requisito fundamental en el desarrollo de las bases de datos, integrada en todas las etapas del diseño, en lugar de ser un requisito aislado y marginal. Se propone una extensión de los modelos de Casos de Uso y de Clases de UML a través de sus mecanismos estándares de extensión (estereotipos, valores etiquetados y restricciones) para poder diseñar bases de datos multinivel. Se realizan las modificaciones necesarias sobre el metamodelo de UML para considerar el nivel de seguridad como un aspecto intrínseco de los elementos de los modelos. Por último se muestra un ejemplo.

Palabras clave: *Bases de datos seguras, UML, restricciones de seguridad, control de acceso, bases de datos multinivel, confidencialidad, diseño de bases de datos.*

1 INTRODUCCIÓN

Los rápidos avances tecnológicos producidos en los últimos años están provocando una mayor utilización de los sistemas de información por parte de las organizaciones (comunicaciones, transporte, banca, educación, fabricación, diseño, medicina, etc.), así como un incremento de la complejidad de los requisitos de información. A menudo, los sistemas de información gestionan una gran cantidad de información que puede ser especialmente importante para la organización, dependiendo la supervivencia de ésta de la correcta gestión, salvaguardia y confidencialidad de esa información. La información que gestionan los sistemas de información es almacenada en las bases de datos y en los datawarehouses, por lo tanto, ellos son puntos clave a la hora de analizar la protección de la información. Por esa razón, la seguridad de las bases de datos es un serio aspecto que debe ser considerado explícitamente, no como un aspecto aislado, sino como un elemento presente en todas las etapas del ciclo de vida de la construcción de la base de datos [14].

En las bases de datos se gestiona y almacena la información relativa a datos bancarios, información judicial, facturas, datos de seguros, información militar, y otros muchos tipos de información valiosa, que ha de ser protegida [6]. A veces, las bases de datos almacenan otro tipo de información que puede ser considerada sensible y que debe estar especialmente protegida ante el acceso a éstas por parte de sujetos no autorizados. Este tipo de información sensible habitualmente se refiere a aspectos íntimos o personales de los individuos, como datos identificativos personales, datos médicos, o incluso creencias religiosas, ideologías o tendencias sexuales [12]. Los sistemas de información que gestionan bases de datos con este tipo de información deberían estar dotados de mecanismos que eviten el acceso no autorizado a la información, garantizando así los derechos de intimidad y privacidad de las personas y el cumplimiento de la *Ley Orgánica de Protección de Datos Personales* [21].

Los problemas de seguridad de la información se agravan como consecuencia de los cambios tecnológicos que están ocurriendo: Acceso a bases de datos a través de la Web, desarrollo del comercio electrónico, avances en los datawarehouses e incluso el uso de técnicas de recuperación de datos como Data Mining [34]. Estos avances hacen, que por ejemplo, los sistemas estén siendo continuamente atacados por hackers [4].

Los argumentos anteriores, que indican la existencia de un serio riesgo sobre los datos almacenados en bases de datos, junto a resultados de estudios como los de [30] que muestran el desinterés de las organizaciones por las seguridad en sus sistemas informáticos (más del 70% de los directivos de las empresas de desarrollo no saben cuando se revisan sus políticas de seguridad) y la escasez de presupuesto dedicado a la seguridad (más del 50% de las compañías dedican menos del 5% de su presupuesto a seguridad, y menos del 5% dedican a seguridad algo más del 15% del presupuesto), demuestran la existencia de grandes vulnerabilidades sobre las bases de datos. Por lo tanto, y puesto que los problemas de seguridad suponen uno de los

frenos al desarrollo de la nueva economía [26], es necesario invertir esfuerzo en el diseño de bases de datos mas seguras.

Todas las iniciativas llevadas a cabo durante los últimos años son muy importantes e indican el gran interés que está suscitando la seguridad de las bases de datos. El problema, es que todas las soluciones que se han dado son soluciones parciales, aisladas e inconexas que no resuelven de una manera global el problema de la protección de las bases de datos, y que además no abordan el problema a nivel de *diseño*. Por ello, proponemos un enfoque metodológico que permita diseñar bases de datos, teniendo en cuenta los aspectos de seguridad desde las etapas más tempranas del desarrollo hasta la finalización del mismo, y que sea una extensión de las metodologías y estándares de modelado existentes en el momento, puesto que de no ser así, las organizaciones realmente interesadas en la seguridad de las bases de datos tendrían que realizar un gran esfuerzo para adaptarse a una nueva metodología.

En estos momentos, el estándar de modelado es UML [5]. De acuerdo a [24] y a [8], UML puede ser utilizado (a través de un proceso adecuado) para el diseño de bases de datos. Por lo tanto parece interesante la idea de dotar a los modelos de UML de características de seguridad para así poder modelar bases de datos seguras. Así, una metodología de diseño de bases de datos basada en el lenguaje UML extendido con aspectos de seguridad, permitiría modelar las bases de datos con la sintaxis y la potencia de UML, y con las nuevas características de seguridad dispuestas para ser utilizadas cuando la aplicación tenga requisitos de seguridad que así lo requieran. Con esto estaríamos cumpliendo las condiciones que impone [9] para diseñar seguridad de la información en los sistemas de manera sistemática, al integrar los requisitos de seguridad en el diseño y al tener disponibles para los diseñadores modelos donde se especifiquen los aspectos de seguridad. Al mismo tiempo estaríamos resolviendo los desafíos que plantean [14] relativos a unificar la seguridad con la ingeniería del software, a la vez que unificamos la seguridad con los modelos del sistema.

2 BASES DE DATOS SEGURAS

A lo largo de la última década han aparecido diversas iniciativas relacionadas con la seguridad en general y algunas concretamente con las bases de datos, como técnicas de análisis y gestión de riesgos [23], técnicas de control de acceso ([7], [15], [18], [20], [28], [35] y [16]), metodologías para el desarrollo de técnicas de seguridad [1], métodos para modelar requisitos de seguridad ([31] y [32]), e incluso alguna metodología para el desarrollo de bases de datos seguras ([22] y [29]). También la ISO/IEC (International Organization for Standarization / International Electrotechnical Commission) ha preparado una guía para la gestión de la seguridad de las tecnologías de Información [19]. A continuación se hace una revisión de algunos de los aspectos más importantes en relación con la seguridad de bases de datos.

Técnicas de Control de Acceso.

El control de acceso es un mecanismo a través del cual aseguramos o tratamos de asegurar que los recursos de información son accedidos sólo por personal autorizado, y que ese personal sólo puede realizar las acciones o actividades autorizadas de acuerdo a su nivel de acreditación dentro del sistema [18].

Habitualmente, el control de accesos a los recursos se realiza utilizando reglas de autorización, que son tuplas con el siguiente formato **<s,o,a>**, que indican que el sujeto **s** puede acceder al objeto **o** realizando la acción **a**. Los tres conceptos que juegan un papel importante en las reglas de autorización son los siguientes:

- Los *sujetos* son las entidades a las que se puede autorizar el acceso a los objetos, y aunque habitualmente son usuarios individuales, también pueden ser grupos de usuarios, roles o incluso procesos que se ejecutan en nombre de los usuarios.
- Los *objetos* son los elementos cuyo acceso queremos controlar. En el caso de sistemas de bases de datos relacionales, los objetos pueden tener distinta granularidad, es decir, se puede acceder a relaciones completas, a vistas, a atributos individuales, etc.
- Las *acciones* son las posibles operaciones que se permiten realizar, y que en bases de datos relacionales habitualmente son la selección, inserción, borrado y actualización.

Existen diversas políticas de control de acceso, algunas de las más importantes son las siguientes:

- Control de Acceso Discrecional. Está basado en la idea de que los sujetos acceden a los objetos en base a su identidad y a unas reglas de autorización que indican para cada sujeto, las acciones que puede realizar sobre los objetos del sistema. Como se indica en [18], este mecanismo de acceso tiene diversas variantes que no tienen por qué ser mutuamente excluyentes. Las más importantes son la autorización positiva y negativa, la autorización fuerte y débil, explícitas e implícitas y basadas en el contenido. Esta política de control de acceso ha sido ampliamente utilizada, pero tiene varias características como la posibilidad de otorgar permisos entre sujetos (dando así la posibilidad de violar la confidencialidad), o la no consideración de unas exigencias mínimas para acceder a los datos dependiendo de sus características, que no la hacen completamente adecuadas para los sistemas de bases de datos actuales, donde los datos tienen sus propias exigencias de confidencialidad, independientemente de los sujetos que deseen acceder a ellos.
- Control de Acceso Obligatorio. Está basado en el modelo diseñado por [3] para sistemas operativos, y consiste en la clasificación de los sujetos y los datos en diversos niveles de seguridad como pueden ser 'sin clasificar', 'confidencial', 'secreto' y 'alto secreto. Así, un dato clasificado en el nivel de seguridad 'alto secreto' sólo podrá ser accedido por sujetos que estén clasificados como 'alto secreto'. Las dos reglas básicas que definen la forma de acceder a los datos mediante esta política, adaptadas al paradigma de las bases de datos, indican que un sujeto tiene acceso de lectura a un objeto si el nivel de acreditación del sujeto domina sobre el nivel de confidencialidad del objeto, y que un sujeto tiene acceso de escritura a un objeto si el nivel de acreditación del sujeto es igual al nivel de seguridad del objeto, es decir, un sujeto solamente puede modificar objetos de su nivel [18].
- Control de Acceso Basado en Tareas. Es apropiado para computación distribuida y para actividades de procesamiento de información con múltiples puntos de control de acceso. Este modelo trata con actividades o tareas para representar las autorizaciones. Se utilizan períodos de tiempo durante los que una autorización permanece válida. La principal idea es otorgar la correcta cantidad de permisos, en el momento adecuado, y sólo aquellas que sean estrictamente necesarias, así como retirar el permiso una vez que sean innecesarias [35].
- Control de Acceso Basado en Roles. Los permisos son asociados con roles, y los usuarios se hacen miembros de esos roles. Los roles representan cada grupo funcional de las organizaciones, agrupando en cada uno de ellos a los usuarios con similares funciones y responsabilidades. A través de este mecanismo es muy sencillo llevar a cabo ciertas acciones como el cambio de usuarios de un rol a otro, así como añadir o eliminar de los roles ciertos permisos según sea necesario. Existen teorías que afirman que el control de acceso obligatorio y el discrecional pueden ser simulados mediante el control de acceso basado en roles [25]. Podemos encontrar un estudio general y nuevas investigaciones sobre esta técnica de control de acceso en [28] y en [15].

Bases de Datos Multinivel.

Las bases de datos multinivel soportan el control de acceso obligatorio a través de diferentes niveles de seguridad en los datos y en los usuarios. Cada nivel de seguridad formará parte de una categoría jerárquica como la ya comentada (alto secreto, secreto, confidencial, no clasificado), o bien podrá pertenecer a una categorías no jerárquicas como finanzas, ventas, investigación, etc. Existen varios prototipos relacionales como SeaView y Lock Data Views, algunos orientados a objetos como SODA , SORION y Jajodia-Kogan, y también algunos productos comerciales como Trudata, Secure Sybase, Trusted Oracle y Trusted Informix [18].

Los objetos que se pueden clasificar en niveles de seguridad, en una base de datos relacional atendiendo a su tamaño o granularidad podrían ser la base de datos entera, tablas, tuplas o bien atributos. Si podemos clasificar las tuplas en distintos niveles de seguridad aparece el problema de la "poli-instanciación", al poder tener varias tuplas con igual clave primaria y distinto nivel de seguridad. El problema se soluciona considerando como clave primaria al resultado de concatenar los atributos que forman la clave primaria con el nivel de seguridad de la tupla. Un análisis en profundidad sobre la poli-instanciación se puede encontrar en [20] y en [7].

A lo largo de estos últimos años han aparecido una serie de arquitecturas para soportar el control de acceso en bases de datos multinivel [18]. Éstas se caracterizan entre otras cosas por la mayor o menor confianza en las medidas de seguridad que aporta el sistema operativo, para así delegar mayor o menor cantidad de aspectos de seguridad en el sistema de gestión de bases de datos.

3 METODOLOGÍAS DE DISEÑO DE SEGURIDAD Y DE DESARROLLO DE BASES DE DATOS

Existen diversas metodologías de desarrollo de bases de datos que generalmente consideran las mismas etapas: Modelado conceptual, diseño lógico y diseño físico ([13], [10] y [2]). Todas estas metodologías no contemplan aspectos de seguridad en sus etapas, motivando el aislamiento de la seguridad y relegándola a un segundo plano.

Por otra parte, también han existido diversos métodos y metodologías para diseñar seguridad. Una clasificación de esas metodologías es la realizada por [1], que considera las tres generaciones siguientes, ninguna de ellas para bases de datos: Métodos de Listas de Control, Métodos de Ingeniería y Transformación Lógica. Una de las pocas metodologías para el diseño de la seguridad de bases de datos es la que aparece en [7], que considera unas fases muy similares a las consideradas en el desarrollo de bases de datos: Análisis preliminar, requisitos y política de seguridad, diseño conceptual, diseño lógico y diseño físico.

Ha existido algún intento no demasiado riguroso de unificar el desarrollo de las bases de datos y la seguridad, como es MOMT (Multilevel Object Modelling Technique) [22]. En MOMT se plantean unas modificaciones sobre OMT (Object Modelling Technique) [27] para soportar niveles de seguridad sobre los elementos de los diagramas de clases, dinámico y funcional.

Para abordar el problema de la seguridad en las bases de datos deberíamos desarrollar una metodología (con "M" mayúscula) [11], que incluya la mayor cantidad de aspectos, como son las personas, los roles, las técnicas, herramientas, procesos, actividades, hitos, productos parciales, estándares, medidas de calidad, etc. considerando en todos ellos a la seguridad.

Como una técnica de esta metodología, ha sido desarrollado un lenguaje de especificación de restricciones de seguridad llamado OSCL (Object Security Constraint Language) [17], que está basado en el lenguaje de restricciones estándar de UML, llamado OCL (Object Constraint Language) [36].

4 EXTENSIÓN DE UML PARA DISEÑAR BASES DE DATOS MULTINIVEL SEGURAS

El objetivo de esta sección es realizar modificaciones en los modelos de casos de uso y de clases de UML para poder diseñar bases de datos multinivel seguras. En la actualidad es aconsejable utilizar lenguajes de modelado orientado a objetos como es UML para diseñar bases de datos [24], puesto que a través de los diagramas de clases se puede recoger a nivel conceptual toda la semántica asociada a una base de datos, incluyendo otros aspectos de la orientación a objetos que no contempla el modelo entidad-interrelación, y que pueden ser importantes para la posterior transformación del modelo conceptual al esquema lógico.

Extensión del Modelo de Casos de Uso.

En los modelos de casos de uso será necesario representar aquellas situaciones en las que un caso de uso requiere una atención especial en relación con la seguridad. En estos casos también habrá que indicar qué actores requieren una cierta acreditación para participar en esos casos de uso.

La extensión del modelo de casos de uso se realiza a través de los estereotipos, creando «*safe-UC*», que se colocará bajo el símbolo del caso de uso. Para los actores que participan en un caso de uso 'seguro' y que requieran tener una cierta acreditación se crea el estereotipo «*accredited-actor*». El motivo de utilizar esta representación es que los diagramas sean fácilmente transportables, condición importante para toda extensión del lenguaje UML. Ver Figura 1.

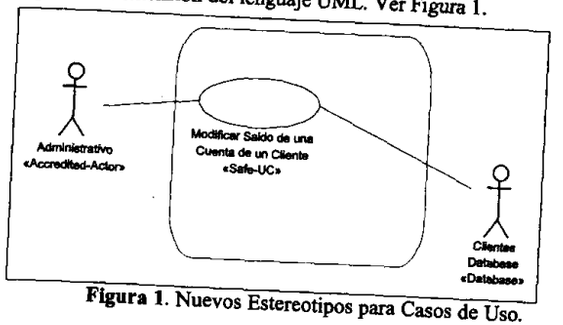


Figura 1. Nuevos Estereotipos para Casos de Uso.

Extensión del Modelo de Clases.

Existen varios tipos de restricciones: Inherentes a un modelo de clases para bases de datos seguras, que no son representadas explícitamente y las definidas por el usuario, que si requieren ser definidas en el modelo. Las principales restricciones inherentes a un modelo son las siguientes:

- Todos los elementos de un modelo tendrán un nivel de seguridad por defecto: el menos restrictivo.
- Todos los objetos tendrán un nivel de seguridad incluido dentro del rango de niveles de seguridad de la clase a la que pertenecen.
- Las asociaciones tendrán un nivel de seguridad, que ha de ser igual o superior al del nivel de las clases que relaciona. De igual forma, una instancia de una asociación tendrá un nivel de seguridad mayor o igual que el de la asociación y que el de los objetos relacionados.
- En una relación de generalización, si se omite el nivel de seguridad de las subclases, éstas heredan el nivel de seguridad de la superclase.
- Como regla general en la relación de generalización, el nivel de seguridad de las subclases ha de dominar o ser más restrictivo que el nivel de seguridad de la superclase, debido al mecanismo de herencia de propiedades.

De acuerdo a la clasificación que realiza [33], podríamos tener los siguientes tipos de restricciones de seguridad definidas por el usuario:

- Simples: Aquellas que clasifican un elemento simple en un nivel de seguridad.
- Basadas en el contenido: Clasifican una parte del modelo dependiendo del valor de algún dato.
- Basadas en eventos: Aquellas que representan el hecho de que el nivel de seguridad de algún elemento del modelo depende de algún acontecimiento externo.
- Basadas en asociación: Asignan un nivel de seguridad a una asociación.
- De agregación: Cuando se clasifica en un cierto nivel de seguridad una agregación de elementos.
- Basadas en niveles: Indican que el nivel de seguridad de cierto elemento depende del nivel de seguridad de otro.
- Lógicas: Cuando especifican implicaciones.
- Meta-restricciones: Son restricciones que clasifican restricciones y metadatos.
- Para poder representarlas se utilizan los siguientes mecanismos de extensión de UML:
- Valores etiquetados: Este tipo de extensión es la utilizada para asignar los niveles de seguridad a los elementos de un diagrama de clases, es decir, para representar restricciones simples y de asociaciones. Algunos ejemplos se muestran en la figura 2 en la que se asignan niveles de seguridad a clases, a atributos y a la asociación entre las clases.

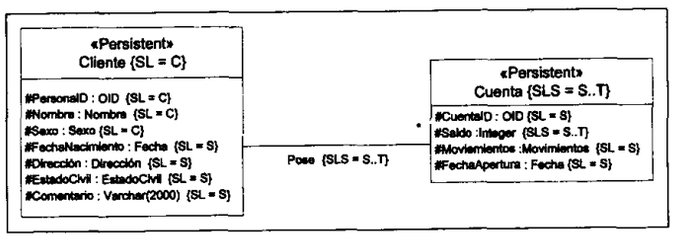


Figura 2. Ejemplo de valores etiquetados.

- Restricciones: Las restricciones se especifican a través del lenguaje OSCL [17] que está especialmente diseñado para especificar restricciones de seguridad. A través de este lenguaje de restricciones se pueden especificar tanto las restricciones inherentes al modelo como el resto de restricciones (a excepción de las basadas en eventos, que se gestionarían desde un modelo dinámico extendido). Un ejemplo es el que aparece en la figura 3, en la que se especifica la restricción de que todas las cuentas de un banco que tengan un saldo superior a 5 millones de pesetas tendrán un nivel de seguridad '*Top Secret*' y el resto '*Secret*'.

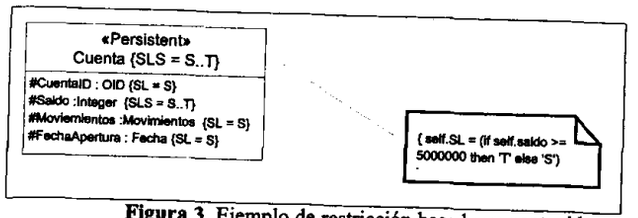


Figura 3. Ejemplo de restricción basada en contenido.

La existencia de valores etiquetados que asignan un nivel de seguridad o rango de niveles de seguridad a los atributos, clases, asociaciones, etc., da pie a pensar sobre la necesidad de modificar el metamodelo, y considerar las propiedades 'nivel de seguridad' y 'rango de niveles de seguridad' como algo inherente a los elementos del modelo, como lo son por ejemplo los atributos para los objetos o el tipo de atributo para los atributos. Así, efectivamente, todos los elementos del modelo de clases tendrán niveles de seguridad, aunque en muchos casos tendrán el valor menos restrictivo por defecto (Sin Clasificar). Las modificaciones del metamodelo son las siguientes:

• Se añaden dos nuevos tipos de datos llamados LEVEL y LEVELS (ver figura 4) que serán los tipos de los atributos que se añadirán a los elementos del modelo para permitir expresar las características de seguridad. El tipo LEVEL indicará el nivel de seguridad de un elemento del modelo. Se considera el tipo LEVELS puesto que a veces los elementos del modelo pueden tener un nivel de seguridad dentro de un cierto rango, que dependerá de determinadas circunstancias como por ejemplo del valor de cierto atributos (restricción basada en contenido).

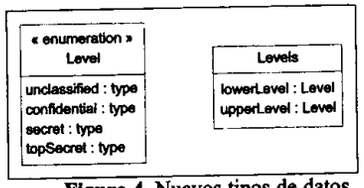


Figura 4. Nuevos tipos de datos.

• En el metamodelo de UML existe una clase llamada '*ModelElement*' que se especializa en todos los elementos del modelo. Puesto que queremos dotar a los elementos del modelo de niveles de seguridad (clases, atributos, instancias, operaciones, métodos, asociaciones y asociaciones de clase, principalmente), la modificación realizada, como podemos apreciar en la figura 5 consiste en añadir unos atributos de seguridad a la clase '*ModelElement*', que heredarán todos los elementos del modelo.

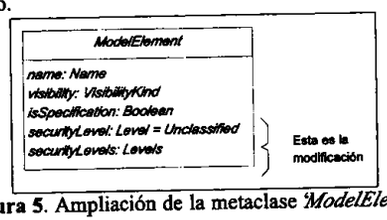


Figura 5. Ampliación de la metaclase '*ModelElement*'.

En la siguiente sección se muestra un ejemplo de modelado en el que se aplican todos los mecanismos de extensión comentados anteriormente para expresar características y restricciones de seguridad.

5 EJEMPLO DE APLICACIÓN DE LA EXTENSIÓN DE UML

Supongamos que deseamos diseñar una base de datos para gestionar una clínica hospitalaria. Para simplificar el problema y poder centrarnos en las características de seguridad hemos considerado solamente algunos de los aspectos importantes que habría que modelar. Un diagrama de casos de uso para este problema sería el que se muestra en la figura 6.

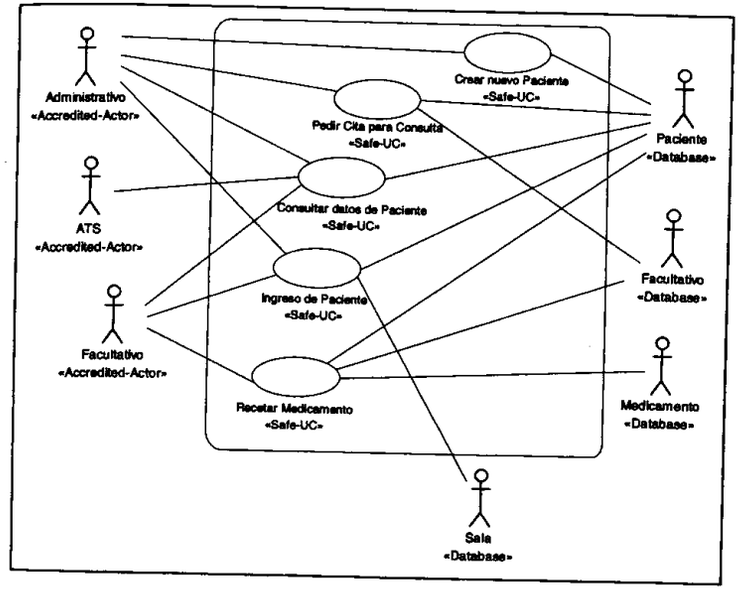


Figura 6. Ejemplo de Diagrama de Casos de Uso.

Podemos observar que en este ejemplo aparece el estereotipo «database» que indica que esos actores almacenarán información que se consultará o modificará en esos casos de uso. Aparece también el estereotipo que identifica casos de uso 'seguros' y el que permite representar actores que necesitarán cierto nivel de acreditación para llevar a cabo los casos de uso.

En las figuras 7 y 8 se muestran varios diagramas parciales pertenecientes al modelo de clases que se ha diseñado para este ejemplo.

En el diagrama de la figura 7 se muestra la jerarquía de personas que integrarán la clínica hospitalaria. Podemos observar que aparecen diversos casos de aplicación de los mecanismos de extensión, como son los valores etiquetados para indicar el nivel o rango de niveles de seguridad de las clases y atributos y las restricciones, que son utilizadas para especificar el nivel de seguridad de ciertos objetos que depende de si se cumple o no una condición sobre el valor de uno de sus atributos. Se puede ver también cómo la herencia no sólo actúa para los atributos y métodos sino también

para los niveles de seguridad. Por ejemplo, la clase Facultativo tiene un rango de niveles de seguridad entre 'Confidencial' y 'Secreto' que es heredado de la clase 'Trabajador'. En este ejemplo se puede observar alguna de las restricciones inherentes al modelo comentadas en el apartado 4.2. como la relativa a los niveles de seguridad entre clases integradas en una relación de generalización (las subclases han de tener un nivel de seguridad más restrictivo que la superclase).

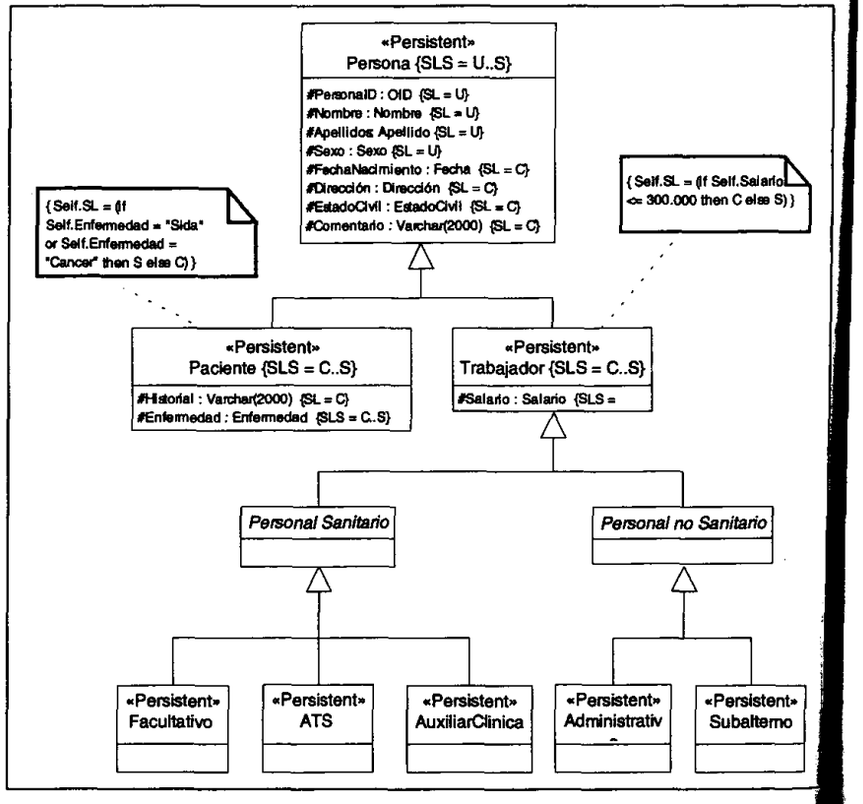


Figura 7. Ejemplo de herencia de niveles de seguridad

En el diagrama de la figura 8 no se ha puesto explícitamente el nivel de seguridad de las asociaciones puesto que no es relevante y porque implícitamente tomaría el rango de niveles de las clases que relacionan. Podemos observar que aparecen algunas clases que no tienen especificado en nivel de seguridad. Esos casos se interpretan como que las clases no tienen ningún requisito de seguridad y por lo tanto, su nivel de seguridad es el que tienen por defecto, es decir, '*Unclassified*'. Las clases que tienen un rango de niveles de seguridad en lugar de un solo nivel de seguridad, indican que su nivel de seguridad depende del nivel de alguno de sus

atributos (por ejemplo el caso del personal laboral, que dependen del nivel salarial), o bien indican que son clases de asociación, donde una de las clases que forma la asociación tiene un rango de niveles de seguridad en lugar de un nivel definido. A veces en el diagrama de objetos no aparece explícitamente el nivel de seguridad de los atributos. En estos casos los atributos heredan el nivel de seguridad especificado para la clase a la que pertenecen.

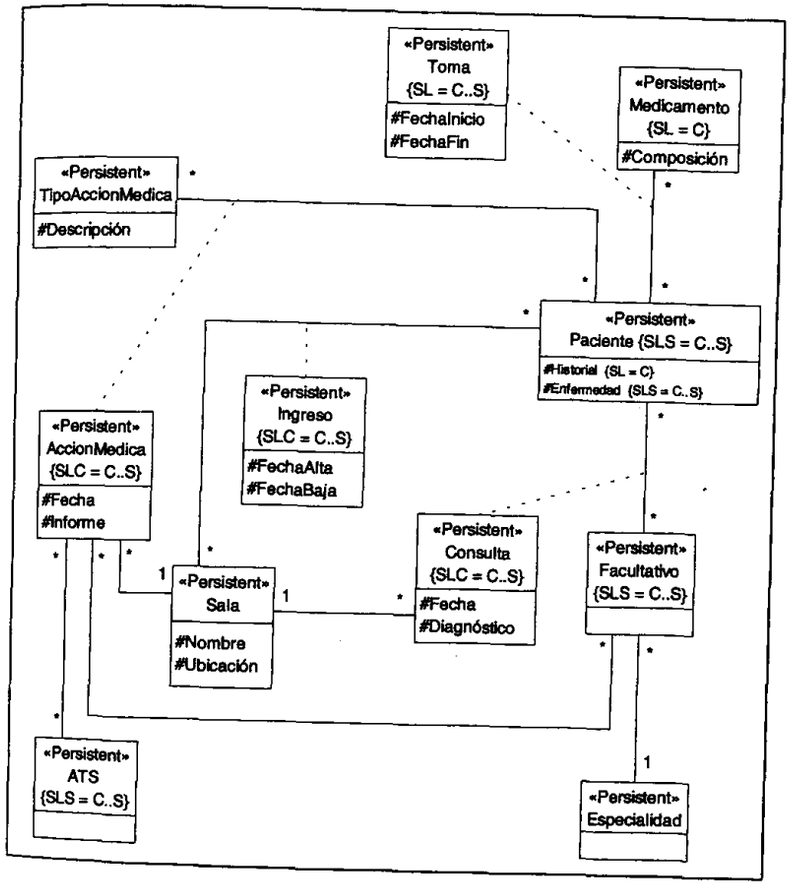


Figura 8. Ejemplo de asociaciones.

6 CONCLUSIONES Y TENDENCIAS FUTURAS.

La seguridad de las bases de datos es un serio problema desde varios puntos de vista, pero sobre todo desde el punto de vista de la confidencialidad, debido a la cada vez mayor importancia que tienen los datos almacenados en ellas. Muchas han sido las soluciones propuestas que han aparecido para el problema de la seguridad en bases de datos, pero todas ellas son parciales y no resuelven el problema de una manera global. En este artículo hemos mostrado que la idea de integrar el diseño de seguridad junto con el diseño de bases de datos es perfectamente factible, y lo hemos hecho extendiendo las características del actual estándar de modelado, UML.

El futuro trabajo se destinará a la creación de una metodología completa para diseñar bases de datos seguras que esté basada en estos modelos extendidos de UML y en el lenguaje diseñado para realizar especificaciones de seguridad (OSCL) y que contemple todos los factores relacionados con el proceso de diseño como herramientas, técnicas, procesos, actividades, hitos, etc.

7 AGRADECIMIENTOS

Este trabajo se ha sido parcialmente financiado por la acción especial 'Red temática española de investigación en el campo de la seguridad de las bases de datos' (TIC 2000-1873-E) y por el proyecto coordinado DOLMEN (TIC2000-1673-C06) del Ministerio de Ciencia y Tecnología, Plan Nacional de I+D+I 2000-2003, Programa de Tecnologías de la Información y de las Comunicaciones.

8 BIBLIOGRAFÍA

1. Baskerville, R. (1993). Information Systems Security Design Methods: Implications for Information Systems Development. *ACM Computing Surveys*. Vol. 25. Nº 4. Diciembre, pp. 375-415.

2. Batini, C., Ceri, S. y Navathe, S. (1992). *Diseño conceptual de bases de datos*. Addison-Wesley / Diaz de Santos.

3. Bell, D. y La Padula, L. (1973). Secure Computer Systems: Mathematical Foundation and Model. *Mitre Corp.*, Beldford, Mass.

4. Bellovin, s. (2001). Computer Security. An end State?. *Communications of the ACM*, Marzo. Vol. 44, Nº 3, pp. 131-132.

5. Booch, G., Rumbaugh, J. y Jacobson, I. (1999). *The Unified Modeling Language*, User Guide. Addison-Wesley, Reading, Mass.

6. Brinkley, D. y Schell, R. (1995). What Is There to Worry About? An Introduction to the Computer Security Problem. *Information Security, An integrated collection of essays*. Eds.: Abrams, M., Jajodia, S. y Podell, H. IEEE Computer Society. California.

7. Castano, S., Fugini, M., Martella, G. y Samarati, P. (1994). *Database Security*. Addison-Wesley.

8. Cabot, J., García, R., Almaleh, Z., Cáceres, P., Marcos, E. y Vázquez, J. (2001). UML en el diseño de bases de datos relacionales. *NOVATICA*. Marzo-Abril. Nº 150. Pp. 62-65.

9. Chung, L., Nixon, B., Yu, E. y Mylopoulos, J. (2000). *Non-Functional Requirements in Software Engineering*. Kluwer Academic Publishers. Boston/Dordrecht/London.

10. Connolly, T., Begg, C. y Strachan, A. (1998). *Database Systems*. Addison-Wesley.

11. Cockburn, A. (2000). Selection a Project's Methodology. *IEEE Software*. Julio-Agosto. Pp. 64-71.

12. Del Peso, E. y Ramos, M.A. (1999). *LORTAD, Reglamento de Seguridad*. Diaz de Santos. Madrid.

13. De Miguel, A., Piattini, M. y Marcos, E. (1999). *Diseño de Bases de Datos Relacionales*. Ra-Ma.

14. Devanbu, P. y Stubblebine, S. (2000). Software Engineering for Security: a Roadmap. *The Future of Software Engineering*. Ed: Finkelstein, A. Pp. 227-239.

15. Ferraiolo, D., Barkley, J. y Kuhn, R. (1999) A role-based access control model and reference implementation within a corporate intranet. *ACM Transactions on Information and Systems Security*. Vol. 2, Nº 1, February 1999, pp. 34-64.

16. Fernández-Medina, E. y Piattini, M. (2001). Security in Database Systems: State of the Art. *Developing Quality Complex Database Systems: Practices, Techniques and Technologies*. Ed. Shirley Becker. Idea Group Publishing.

17. Fernández-Medina, E., Piattini, M. y Serrano, M. A. (2001). Specification of Security Constraints in UML. Actas de *35th Annual 2001 International Carnahan Conference on Security Technology*. Londres.

18. Ferrari, E. y Thuraisingham, B. (2000). Secure Database Systems. *Advanced Databases: Technology Design*. Eds.: Piattini, M. y Díaz, O. Artech House. Londres.

19. ISO/IEC TR 13335 (1997). *Information technology- Guidelines for the management of IT Security*.

20. Jajodia, S, Sandhu, R. y Blaustein, B. (1995). Solutions to the Polyinstantiation Problem. *Information Security, An integrated collection of essays*. Eds.: Abrams, M., Jajodia, S. y Podell, H. IEEE Computer Society. California.

21. *Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.* BOE núm 298, de 14 de diciembre de 1999.

22. Marks, D., Sell, P. y Thuraisingham, B. (1996). MOMT: A multilevel object modeling technique for designing secure database applications. *Journal of Object-Oriented Programming*. Vol. 9. Nº 4, pp. 22-29.

23. MAP (1996). *Metodología de Análisis y Gestión de Riesgos del Ministerio de Administraciones Públicas Español*, MAGERIT v.1.0

24. Muller, R. (1999). *Database Design for Smarties. Using UML for Data Modeling*. Morgan Kaufmann Publishers, inc. San Francisco, California.

25. Osborn, S., Sandhu, R. y Munawer, Q. (2000). Configuring Role-Based Access Control to Enforce Mandatory and Discretionary Access Control Policies. *ACM Transactions on Information and System Security,* Vol. 3, Nº 2, Mayo, Pp: 85-106.

26. Palau, M. (2001). ¿Calidad de la seguridad o seguridad de la calidad?. *SIC: Seguridad en Informática y Comunicaciones.* Abril. Nº44. Pp. 30-32.

27. Rumbaugh, J., Blaha, M, Premerlani, W., Eddy, F. y Lorensen, W. (1991). *Object-Oriented Modeling and Design.* Prentice Hall, Englewood Cliffs.

28. Sandhu, R. y Bhamidipati, V. (1997). The URA97 model for role-based user-role assignment, in *Database Security XI: Status and Prospects*. Eds.: T.Y. Lin y S. Qian. Chapman and Hall, London, pp. 262-275.

29. Sell, P. y Thuraisingham, M.B. (1993). Applying OMT for Designing Multilevel Database Applications. Actas *de Seventh IFIP Working Conference on Database Security*. Huntville, Septiembre.

30. SIC (2001). *Seguridad en Informática y Comunicaciones*. Abril. Nº 44. P. 6.

31. Smith, G.W. (1990). The Semantic Data Model for Security: Representing the Security Semantics of an Application. Actas de *the Sixth International Conference Data Engineering*, IEEE, pp. 322-329.

32. Smith, G.W. (1991). Modeling Security-Relevant Data Semantics. Actas de *IEEE Transactions on Software Engineering*, Vol. 17. Nº 11, Noviembre, pp. 1195-1203.

33. Thuraisingham, B. y Ford, W. (1995). Security Constraint Processing in a Multilevel Secure Distributed Database Management System. *IEEE transactions on knowledge and data engineering,* Vol 7. Nº 2. Abril. Pp. 274-293.

34. Thuraisingham, B., Schlipper, L., Samarati, P., Lin, Jajodia, S. y Clifton, C. (1997). Security issues in data warehousing and data mining: panel discussion, *in Database Security XI: Status and Prospects*. (eds. T.Y. Lin y S. Qian), Chapman and Hall, London, pp. 3-16.

35. Tomas, R. y Sandhu, R. (1997). Task-based authorization controls (TBAC): a family of models for active and enterprise-oriented authorization management, *in Database Security XI: Status and Prospects*. (eds. T.Y. Lin y S. Qian), Chapman and Hall, London, pp. 166-181.

36. Warmer, J. y Kleppe, A. (1998). *The object constraint language.* Massachusetts. Addison-Wesley.