Curriculum Vitae

Dr. José Ramón Coz Fernández

Abril 2025

Tabla de contenido

INFORMACIÓN PERSONAL 3
BREVE RESUMEN CURRICULAR 3
EXPERIENCIA PROFESIONAL 4
ESTUDIOS Y FORMACIÓN 7
DOCTORADO 7
LICENCIATURAS Y MÁSTER 8
ESTUDIOS DE POST-GRADO 8
CERTIFICACIONES PROFESIONALES 9
CURSOS SOBRE SEGURIDAD, DEFENSA Y ESPACIO 12
OTROS CURSOS 15
IDIOMAS 15
ACTIVIDAD INVESTIGADORA 16
ARTÍCULOS Y PUBLICACIONES 16
PONENCIAS EN CONFERENCIAS Y CONGRESOS 22
LIBROS Y CAPÍTULOS DE LIBROS 26
COLABORACIÓN CON GRUPOS, REVISTAS Y PUBLICACIONES 29
PATENTES - REGISTRO DE LA PROPIEDAD INTELECTUAL 29
ENLACES SOBRE ACTIVIDAD CIENTÍFICA E INVESTIGADORA 30
ACTIVIDAD DOCENTE 32
ASIGNATURAS Y CURSOS IMPARTIDOS 32
ESTANCIAS COMO PROFESOR VISITANTE 33
PROGRAMAS UNIVERSITARIOS DE RADIO 34
DIRECCIÓN DE TRABAJOS FIN DE MASTER 34
ASISTENCIA A TRIBUNALES UNIVERSITARIOS 36
PROYECTOS DE INNOVACIÓN DOCENTE 37
OTROS DATOS DE INTERES 37
MEMBRESÍAS 37
PERFILES EN REDES SOCIALES 37

INFORMACIÓN PERSONAL

Nombre	**Dr. D. JOSE RAMON COZ FERNANDEZ**
Teléfono	+31 71 565 57 57, +34 649 18 43 37
E-mail	jose.ramon.coz@esa.int
Nacionalidad	ESPAÑOLA
Fecha de nacimiento	16 – 06 – 1972
Web	http://www.cozweb.es/
Perfil LinkedIn	es.linkedin.com/in/jrcoz
Perfil Investigador	www.researchgate.net/profile/Jose_Coz

BREVE RESUMEN CURRICULAR

José Ramón Coz es **Doctor cum laude en Economía** por la Universidad Complutense de Madrid y **Doctor cum laude en Ingeniería Informática** por la Universidad Nacional de Educación a Distancia (UNED).

Además, es **Licenciado en Ciencias Físicas** por la Universidad de Cantabria, Grado **Máster en Economía** por la Universidad Complutense de Madrid, Graduado Especialista en Gestión Pública por la Universidad Politécnica de Madrid y Master en Dirección de Tecnologías de la Información por el IDE-CESEM.

Posee más de 20 certificaciones internacionales en Tecnologías de la Información y varios postgrados en Telecomunicaciones.

Tiene más de **25 años de experiencia en Tecnologías de la Información y las Comunicaciones, y más de veinte años de experiencia en el campo de la Ciberseguridad.**

En la actualidad, es el **responsable de las Auditorias de Ciberseguridad en el Directorado de Navegación de la Agencia Espacial Europea**, es **investigador** en el Departamento de Economía Aplicada de la Universidad Complutense de Madrid y **profesor** en varias instituciones, universidades y escuelas de negocio.

Ha realizado varias publicaciones científicas y de tecnología, es revisor y miembro del comité editorial de varias revistas internacionales de ciencia, economía y tecnología, y miembro de varias comisiones y asociaciones de auditoría y tecnologías de la información.

EXPERIENCIA PROFESIONAL

Más de 25 años de experiencia profesional en el campo de las Tecnologías de la Información, la Seguridad y la Auditoria en diversas instituciones públicas y privadas como la Agencia Espacial Europea, la OTAN, el Ministerio de Justicia, el Ministerio de Defensa, el Cuerpo Nacional de Policía, Fomento de Construcciones y Contratas y varias entidades bancarias.

Fecha (desde – a)	**Octubre de 2018 hasta la actualidad**
Nombre del contratista	**EUROPEAN SPACE AGENCY.** ESTEC. NOORDWIJK, PAISES BAJOS.
Cargo y nombre del puesto	**CYBER INTERNAL AUDITS HEAD**
Principal actividad y responsabilidades	• Funcionario de la Agencia Espacial Europea. • *Cyber Internal Audits Head* en el Directorado de Navegación. • El rol principal lo establece la Política Cibernética de la Comisión Europea. • Responsable de realizar auditorías de seguridad cibernética, incluida la evaluación del nivel de cumplimiento del sistema de gestión de seguridad de la información y las medidas de seguridad implementadas. • Esta función tiene una línea de reporte directa al Director de Navegación, y cubre programas por un alcance de más de un billón de euros anuales y la coordinación del trabajo de más de cuarenta (40) empresas.

Fecha (desde – a)	**Marzo de 2012 hasta la octubre 2018**
Nombre del contratista	**NATO COMMUNICATIONS AND INFORMATION AGENCY (NCIA).** BRUSELAS, LA HAYA. Contratado a través de **ISDEFE**, empresa pública del Ministerio de Defensa.
Cargo y nombre del puesto	**AUDITOR Y RESPONSABLE DEL SOPORTE DEL SERVICIO DE CIBERSEGURIDAD EN LA OFICINA PMIC DE LA OTAN**
Principal actividad y responsabilidades	• Auditor independiente del portafolio de proyectos de ciberseguridad y gestionados por la NATO Communications and Information Agency (NCIA). Se trata de proyectos de más de 400 M€, que se implantan en más de 30 países y que conllevan el desarrollo, diseño, implantación y gestión de las principales cibercapacidades de la OTAN. Esta labor conllevaba la monitorización de la implementación de todos los proyectos en sus ámbitos técnicos, de aseguramiento de la calidad, financieros y de contratación. • Responsable del Servicio de Soporte a la Ciberseguridad en la Oficina de Gestión e Integración de Programas (PMIC) de la NATO Communications and Information Agency (NCIA). La PMIC daba soporte a diversos programas de tecnología de la OTAN a través de servicios de auditorías independientes, gestión de riesgos, configuración, cambios, y requisitos, arquitecturas, gestión contractual y de costes. • **NATO MERIT AWARD 2013**. Premio otorgado por OTAN en noviembre de 2013 por el trabajo realizado durante 20 meses para el despliegue de diversas cibercapacidades de OTAN en más de veinte países.

Fecha (desde – a)	**Octubre de 2009 hasta febrero 2012**
Nombre del contratista	**SECRETARIA DE ESTADO DE DEFENSA**. Contratado a través de **ISDEFE**, empresa pública del Ministerio de Defensa.
Cargo y nombre del puesto	**GABINETE DE LA VICEPRESIDENCIA DE ISDEFE**
Principal actividad y responsabilidades	• Apoyo al desarrollo y difusión de la Política Industrial del Ministerio de Defensa. • Participación en grupos de trabajo de apoyo a la Secretaría de Estado de Defensa, en los ámbitos de Ciberseguridad, Auditoría y Tecnología. • Estudios y proyectos de investigación económicos, Industriales y Estratégicos sobre el Sector Industrial de la Defensa. • Colaboración con la Cátedra de Mercados y Política Industrial de Isdefe con el Instituto de Economía de Barcelona.

Fecha (desde – a)	**Noviembre de 2008 hasta octubre 2009**
Nombre del contratista	**SUBDIRECCIÓN GENERAL DE REGISTROS DE APOYO A LA ACTIVIDAD JUDICIAL. MINISTERIO DE JUSTICIA.** Contratado a través de **ISDEFE**, empresa pública del Ministerio de Defensa.
Cargo y nombre del puesto	**CONSULTORÍA Y ASESORAMIENTO EN GESTIÓN DE PROGRAMAS**
Principal actividad y responsabilidades	• Gestión de Proyectos y Consultoría Estratégica en el Plan de Modernización del Ministerio de Justicia. • Apoyo a la subdirección General de Registros de Apoyo a la Actividad Judicial en materia de Tecnologías de la Información. Metodologías y Buenas Prácticas de Gestión de Proyectos. PRINCE2, COBIT, NIST, ISO27, VALIT, ITIL. • Control y Seguimiento de la Evolución de los sistemas corporativos Judiciales. gestión del cambio. • Interlocución con las empresas y Entidades responsables del desarrollo y Mantenimiento de los sistemas. • Gestión de los Contratos de Nivel de Servicio (SLA, SLM). • Responsable y colaborador en la elaboración de ofertas para Proyectos Internacionales (Comisión Europea, OTAN y Naciones Unidas)

Fecha (desde – a)	**Noviembre de 2005 hasta noviembre 2008.**
Nombre del contratista	**CUERPO NACIONAL DE POLICIA. ÁREA DE INFORMÁTICA.** Contratado a través de **ISDEFE**, empresa pública del Ministerio de Defensa
Cargo y nombre del puesto	**ASESOR DE SEGURIDAD TIC Y GESTIÓN DE PROYECTOS.**

Principal actividad y responsabilidades	• Colaborador como Experto en varios Proyectos:
	  o Infraestructuras Críticas de Seguridad en España. Proyecto para la Comisión Europea.
	  o Gestión de la Identidad digital (Seguridad 2020). Proyecto de I+D del Ministerio de Industria.
	  o Proyectos Internacionales Clasificados de Seguridad en Inmigración, Gestión de Fronteras y gestión de Identidades.
	• Miembro de la Oficina de Dirección del DNI Electrónico y el Pasaporte Electrónico (proyectos de más de 200 M€):
	  o Asesoramiento en la gestión del proyecto y control de la calidad.
	  o Convenios Marco con otras instituciones como el MAP, Ministerio de Industria, Agencia Tributaria o la Fábrica de Moneda y Timbre.
	  o Colaboración en las Auditorías de Seguridad y LOPD, y acreditaciones (CNI / CNN / ITSEC).
	• Apoyo al Servicio de Gestión de Proyectos del área de Informática del Cuerpo Nacional de Policía. Gestión Técnica de Proyectos.
	• Estudio de Funciones TI en la Policía y asesoramiento en la implantación de las mejores prácticas (ITIL, COBIT, PRINCE2, NIST, ISO27).

Fecha (desde – a)	**Enero de 2005 a noviembre 2005**
Nombre del contratista	**INSPECCIÓN GENERAL CIS DEL MINISTERIO DE DEFENSA** Contratado a través de **ISDEFE**, empresa pública del Ministerio de Defensa
Cargo y nombre del puesto	**RESPONSABLE TÉCNICO DEL PROYECTO PLAN DE CONTINUIDAD DEL CENTRO DE OPERACIÓN Y APOYO DEL MINISTERIO DE DEFENSA.**
Principal actividad y responsabilidades	• Dirección técnica del proyecto PLAN DE CONTINUIDAD DEL CENTRO DE EXPLOTACION Y APOYO (CCEA) del Ministerio de Defensa. El proyecto tenía un alcance de más de 400 sistemas de información. • Análisis de Impacto. • Elaboración de Procedimientos y Planes de Emergencia. • Diseño de Centros de Respaldo. • Implementación de nuevas prácticas COBIT, ITIL, NIST, ISO27 y Normativas OTAN

Fecha (desde – a)	**Enero 2003 a enero 2005**
Nombre del contratista	**INSPECCIÓN GENERAL CIS DEL MINISTERIO DE DEFENSA** Contratado a través de **ISDEFE**, empresa pública del Ministerio de Defensa
Cargo y nombre del puesto	**CONSULTOR EN ARQUITECTURA DE SISTEMAS Y SEGURIDAD**
Principal actividad y responsabilidades	• Asesor del Ministerio de Defensa en materia de adquisiciones CIS. Estimación Económica, toma de decisiones y control y seguimiento de las adquisiciones. Elaboración de Normativas CIS relacionadas con la seguridad de la información. • Gestión y supervisión de los estudios de Mercado de Productos. • Gestión y supervisión de la entrada en explotación de diversos sistemas de Información del Ministerio. • Responsable de la Elaboración y Difusión de la Arquitectura Técnica. • Colaboración con grupos OTAN de Arquitecturas Software. • Colaboración con la Oficina de Datos del Ministerio de Defensa: • Política de Datos del Ministerio. • Guías de Uso y Normativas de Datos. • Comité de Seguimiento del Centro Internacional de Desminado.

Fecha (desde – a)	**Mayo 2000 a marzo 2003**
Nombre del contratista	**CONSORCIO EUROFIGHTER**, Contratado a través del **GRUPO DE FOMENTO CONSTRUCCIONES Y CONTRATAS (FCC).** DIVISION ESPELSA STC.
Cargo y nombre del puesto	**ANALISTA DE SISTEMAS Y SEGURIDAD.**
Principal actividad y responsabilidades	• Analista en los Proyectos MPB y MDB (Sistemas de Planificación, Debriefing y Briefing de Misiones Aéreas), liderados por ESPELSA y formados por el Consorcio Internacional EUROFIGHTER (THALES – inglés, GALILEO –italiano, DORNIER –alemán, CASA –español). Proyectos clasificados. • Analista en los Proyectos: MPDS (Planeamiento de Misiones para los aviones del Ejército del Aire), Módulos de Carga de Datos para el ORION P3 y Administración del MACOM para el Ejército del Aire. Proyectos Clasificados, en participación con INDRA y CASA. Gestión de equipos de Programación. • Responsable de las Certificaciones de Seguridad (ITSEC).

Fecha (desde – a)	**Noviembre 1999 a mayo 2000**
Nombre del contratista	**ARGENTARIA**. Contratado a través del **GRUPO ABS.**
Cargo y nombre del puesto	**CONSULTOR SENIOR DE SISTEMAS**

Principal actividad y responsabilidades	• Consultoría y Análisis de Proyectos de Sistemas de la Información para el Grupo Argentaria.
	• Participación como analista y consultor de ciberseguridad en los Proyectos:
	  o INTRANET de Argentaria.
	  o Optimización de Bases de Datos.
	  o Proyecto Gestión de Tarjetas Bancarias y Proyecto SIPYC.
	• Análisis de Bases de Datos Dimensionales.

Fecha (desde – a)	**Marzo 1998 a noviembre 1999**
Nombre del contratista	**CAJA ESPAÑA**. Contratado a través del **GRUPO IBV.** CENTRISA (actualmente forma parte de la empresa INDRA). (LEÓN)
Cargo y nombre del puesto	**CONSULTOR DE SISTEMAS**

Principal actividad y responsabilidades	• Consultoría, Análisis y desarrollo de Proyectos de Tecnología de Sistemas para Caja España. Participación en los Proyectos:
	  o Cuentas de Crédito a Promotores.
	  o Intranet bajo tecnología Lotus Notes.
	• Migración a Java de las Aplicaciones Corporativas.
	• Migración al Euro de las aplicaciones del Departamento de Pasivo.

Fecha (desde – a)	**Octubre 1997 a marzo 1998**
Nombre del contratista	**IDEAL OBJECTS. S. A**
Cargo y nombre del puesto	**ADJUNTO A LA DIRECCIÓN COMERCIAL**
Principal actividad y responsabilidades	• Soporte a Grandes Empresas de las Librerías de Software que distribuía la Empresa: Librerías de Java y C++. • Soporte de Entornos CORBA. • Soporte de Bases de Datos Orientadas a Objetos (Object Store). • Soporte Técnico a la venta.

Fecha (desde – a)	**Marzo 1997 a octubre 1997**
Nombre del contratista	**INSTITUTO ESPAÑOL DE FOMENTO INDUSTRIAL (IEFI).**
Cargo y nombre del puesto	**INGENIERO DE SOPORTE**
Principal actividad y responsabilidades	• Soporte Técnico. • Apoyo técnico a la actividad comercial del Instituto. • Diseño y formación sobre Productos de Bases de Datos a través de Internet. • Consultoría sobre Sistemas Operativos, Navegadores y Mensajería electrónica.

ESTUDIOS Y FORMACIÓN

Doctor en Economía, Doctor en Ingeniería Informática, Grado Master en Economía, Licenciado en Ciencias Físicas, diversos postgrados en Telecomunicaciones, Grado Especialista en Gestión de las Administraciones Públicas, Máster en Dirección de Sistemas de Información, **y más 20 certificaciones profesionales internacionales** como CISA, CISM, CGEIT, CRISC, ITIL, COBIT, MSP, PRINCE2 o ISO20000.

DOCTORADOS

Fecha (desde – a)	SEPTIEMBRE 2012 – ABRIL 2016
Nombre de la Universidad	**Universidad Complutense de Madrid. Facultad de Ciencias Económicas y Empresariales.**
Estudios principales (o campo de trabajo)	Doctorado en Economía. Desde 2012 colaboro como Investigador en el Departamento de Economía Aplicada VI de la Facultad de Ciencias Económicas y Empresariales de la Universidad Complutense de Madrid. Los campos de la investigación son la Economía Pública Avanzada y los Modelos de Eficiencia Avanzados en el Gasto Publico. Tesis Doctoral: *"Modelo de Gestión del Conocimiento para el Impacto Económico. Aplicación al sector Defensa."*
Título o Certificado	**DOCTOR EN ECONOMIA con la calificación de Sobresaliente Cum Laude.**

Fecha (desde – a)	SEPTIEMBRE 2006 A MAYO 2011
Nombre de la Universidad	**Departamento de Ingeniería del Software y Sistemas Informáticos. ETS Ingeniería Informática. UNED**
Estudios principales (o campo de trabajo)	Doctorado en Ingeniería Informática. Investigador en el Departamento de Ingeniería del SW y Sistemas en la UNED durante más de 5 años. Campos de la investigación: seguridad de la información, bases de datos, programación generativa, modelos económicos y líneas de productos software. Tesis Doctoral: *"Desarrollo de un servicio de notificación de cambios en una base de datos de gestión de la configuración mediante programación generativa"*
Título o Certificado	**DOCTOR EN INGENIERIA INFORMÁTICA con la calificación de Sobresaliente Cum Laude.**

LICENCIATURAS Y MÁSTER

Fecha (desde – a)	SEPTIEMBRE 2011 A SEPTIEMBRE 2012
Nombre de la Universidad	Universidad Complutense de Madrid. Facultad de Económicas.
Estudios principales	Máster Oficial en Economía. Especialidad en Logística y Economía de la Defensa.
Título o Certificado	**MÁSTER UNIVERSITARIO EN LOGÍSTICA Y GESTIÓN ECONÓMICA DE LA DEFENSA.** ESPECIALIDAD DIRECCIÓN FINANCIERA Y CONTRATACIÓN. NOTA: Seleccionado en el Top 20 del Ranking Mundial de Masters en Logística y Gestión Económica en el año 2012.

Fecha (desde – a)	SEPTIEMBRE 1990 A SEPTIEMBRE 1995
Nombre de la Universidad	**UNIVERSIDAD DE CANTABRIA. Facultad de Ciencias.**
Estudios principales	Licenciatura en Ciencias Físicas. Especialidades en Electrónica y Computación.
Título o Certificado	**LICENCIADO EN CIENCIAS FÍSICAS. ESPECIALIDAD ELÉCTRONICA Y COMPUTADORES.**

ESTUDIOS DE POST-GRADO

Fecha (desde – a)	SEPTIEMBRE 2003 A JUNIO 2005
Nombre de la Universidad	**CEPADE**. **Universidad Politécnica de Madrid.**
Estudios principales	• Sistemas de Información aplicados a las Administraciones Publicas. • Métodos de Planificación y Control en la Administración Pública. • Diseño e Implantación de Proyectos de e-administración. • Gestión de los Recursos Humanos en las Administraciones Públicas. • Gestión de Proyectos Tecnológicos. Gestión de Sistemas de Información. • Fundamentos de Métodos Cuantitativos para la Economía y la Empresa.
Título o Certificado	**GRADUADO ESPECIALISTA EN GESTION DE LA ADMINISTRACION PÚBLICA**

Fecha (desde – a)	SEPTIEMBRE 2001 A SEPTIEMBRE 2003
Nombre de la Entidad	**IDE – CESEM**. **Instituto de Directivos de Empresa.**
Estudios principales (o campo de trabajo)	• Software Orientado a Objetos. Sistemas de Ayuda a la Decisión. • Seguridad Informática. Los Sistemas de la Información. • Habilidades Directivas. Gestión Financiera y Económica. • Gestión de Recursos Humanos del Departamento de Informática. • Explotación y Control. E – Business. Dirección y Gestión de Proyectos. • Dirección de Equipos. Desarrollo de Sistemas. • Comunicaciones y Comunicaciones Avanzadas. Auditoria. • Proyecto Fin de Máster: *"Modelo Tecnológico y Normativo para una gran Corporación"*.
Título o Certificado	**MÁSTER DE DIRECCION DE TECNOLOGIAS DE LA INFORMACION** (600 Horas). 2º en el ranking de Máster de Tecnología por el estudio del diario el Mundo en el año 2004.

Fecha (desde – a)	SEPTIEMBRE 2002 A JUNIO 2003
Nombre de la Universidad	**Escuela Superior de Ingenieros de Telecomunicación**. **Universidad Politécnica de Madrid**.
Estudios principales (o campo de trabajo)	• Seguridad en Redes de Telecomunicaciones. • Sistemas y Redes de Comunicaciones TCP/IP. • Sistemas Distribuidos en Web.
Título o Certificado	**POST-GRADOS en SISTEMAS DE REDES Y COMUNICACIONES PARA LA SEGURIDAD Y LA DEFENSA.**

CERTIFICACIONES PROFESIONALES

Date	OCTOBER 2021
University or Centre	**Teaching Science and Technology, Inc. (USA)**
Studies	• Space Systems Engineering • Satellite Hardware Laboratory Areas and Activities (EyasSAT) • Validating Requirements & Models of Satellites • Verifying Satellite Products • Verification of COTS/NDI • Satellite Software Verification & Validation • Validating Products and Flight Certification
Certificate	**SPACE SYSTEM VERIFICATION AND VALIDATION**

Date	JUNE 2020
University or Centre	**Teaching Science and Technology, Inc. (USA)**
Studies	• Designing Space Missions & Systems • Space System Operations • Mission Management. • Analyze proposed mission designs with insight into the critical trade-offs between cost, schedule, performance and risk.
Certificate	**DESIGNING SPACE MISSIONS & SYSTEMS**

Fecha de Obtención	ABRIL 2016
Nombre de la Entidad	**Club BPM (Business Process Management)**
Estudios principales (o campo de trabajo)	• Análisis, Diseño, Modelización e Implementación ágil de sistemas, a través del estándar BPM. • Alineación estratégica e Inteligencia Operacional.
Título o Certificado	**CERTIFICACIÓN PROFESIONAL INTERNACIONAL: BPM: RAD®-C**

Fecha de Obtención	NOVIEMBRE 2013
Nombre de la Entidad	**Agencia Española de Certificaciones de Ciberseguridad (ACC)**
Estudios principales (o campo de trabajo)	• Seguridad física del entorno y los soportes. Seguridad de los sistemas • Seguridad de las operaciones. Seguridad de los ficheros • Seguridad del personal.
Título o Certificado	**CERTIFICACIÓN CIBERSEGURIDAD – CONCIENCIACIÓN Y SENSIBILIZACIÓN EN SEGURIDAD (CCS-S)**

Fecha de Obtención	NOVIEMBRE 2013
Nombre de la Entidad	**Agencia Española de Certificaciones de Ciberseguridad (ACC)**
Estudios principales (o campo de trabajo)	• Criptografía y esteganografía • Sistemas de autenticación y control de acceso • Seguridad perimetral • Seguridad de las comunicaciones • Seguridad en sistemas operativos • Seguridad en redes inalámbrica
Título o Certificado	**CERTIFICACIÓN CIBERSEGURIDAD – TECNOLOGÍA SEGURIDAD CCS-T**

Fecha de Obtención	JUNIO 2010
Nombre de la Entidad	**APM GROUP**
Estudios principales (o campo de trabajo)	• Estrategia de los Servicios TIC. Diseño de los Servicios TIC • Transición de Servicios TIC. Operación de Servicios TIC • Mejora Continua. ISO 20000 y Novedades de ITIL V3.
Título o Certificado	**ITIL Foundation V3 Bridge**

Fecha de Obtención	JULIO 2010
Nombre de la Entidad	**Asociación Profesional Española de Privacidad**
Estudios principales (o campo de trabajo)	• Conceptos Jurídicos de la Privacidad. La LOPD. • Conceptos Técnicos sobre la Privacidad. • Reglamentación en ámbitos sectoriales. • Procedimientos administrativos de protección de datos.
Título o Certificado	**ACP CONSULTANT**

Fecha de Obtención	SEPTIEMBRE 2010
Nombre de la Entidad	**ISACA (Information Systems Audit and Control Association)**
Estudios principales (o campo de trabajo)	• Risk Identification, Assessment and Evaluation • Risk Response and Risk Monitoring • IS Control Design and Implementation • IS Control Monitoring and Maintenance
Título o Certificado	**CERTIFIED IN RISK AND INFORMATION SYSTEMS CONTROL – IT (CRISC)**

Fecha de Obtención	OCTUBRE 2009 y renovado en NOVIEMBRE 2013.
Nombre de la Entidad	**OPEN GROUP**
Estudios principales (o campo de trabajo)	• Architecture Development Methods • Architecture Content Framework • Enterprise Continuum & Tools • Foundation Architecture - TRM and III-RM • Architecture Capability Framework **TOGAF V8 CERTIFIED**

Fecha de Obtención	SEPTIEMBRE 2009
Nombre de la Entidad	**APMG (AMP Group)**
Estudios principales (o campo de trabajo)	• Use of Managing Successful Programs (MSP) • Programme Management : profiles, documentation, processes, activities, and techniques. • Transformational Flow in programs. • Program Office Management
Título o Certificado	**MSP PRACTITIONER**

Fecha de Obtención	SEPTIEMBRE 2009
Nombre de la Entidad	**APMG (AMP Group)**
Estudios principales (o campo de trabajo)	• Managing Successful Programs (MSP). • Theory: Principles and Themes. • Program Management Theory: profiles, documentation, processes, and activities. Transformational Flow Theory.
Título o Certificado	**MSP FOUNDATIONS**

Fecha de Obtención	JULIO 2009
Nombre de la Entidad	**ISACA (Information Systems Audit and Control Association)**
Estudios principales (o campo de trabajo)	• How IT management issues are affecting organizations • Control framework driven by IT Governance. • How COBIT meets the requirement for an IT Governance Framework • How COBIT is used with other standards and best practices • The COBIT Framework and all the components of COBIT • How to apply COBIT in a practical situation.
Título o Certificado	**COBIT FOUNDATIONS**

Fecha de Obtención	JUNIO 2008
Nombre de la Entidad	**APM Group**
Estudios principales (o campo de trabajo)	• Modelo Avanzado de Procesos de Gestión de Proyectos PRINCE2 (Project In Control Environments), Aplicación de PRINCE2 en proyectos. • Utilización de los Componentes, Roles, Herramientas, Técnicas y Plantillas propuestos por PRINCE2 en proyectos.
Título o Certificado	**PRINCE2 PRACTITIONER**

Fecha de Obtención	MARZO 2008
Nombre de la Entidad	**EXIN (Examination Institute for Information Science)**
Estudios principales (o campo de trabajo)	• Gestión de Incidentes y Problemas. • Gestión de Configuración y Cambios. Gestión de Versiones. • Gestión de la Disponibilidad, Continuidad y la Capacidad. • Administración y Estimación Financiera. • Gestión de Niveles de Servicios. Gestión de Proveedores y Clientes.
Título o Certificado	**ISO 20000 FOUNDATIONS**

Fecha de Obtención	FEBRERO 2008
Nombre de la Entidad	**ISACA (Information Systems Audit and Control Association)**
Estudios principales (o campo de trabajo)	• Strategic Alignment • Value Delivery • Risk Management and Resource Management • Performance Measurement
Título o Certificado	**CERTIFIED IN THE GOVERNANCE OF ENTERPRISE IT (CGEIT)**

Fecha de Obtención	OCTUBRE 2007
Nombre de la Entidad	**SEI (Software Engineering Institute)**
Estudios principales	Modelo de Madurez CMMI
Título o Certificado	**CURSO OFICIAL DEL SEI SOBRE CMMI**

Fecha de Obtención	ABRIL 2007
Nombre de la Entidad	**APMG (AMP Group)**
Estudios principales (o campo de trabajo)	• Modelo de Procesos de Gestión de Proyectos PRINCE2 (Project In Control Environments) • Los Componentes y los Roles en Gestión de Proyectos PRINCE2 • Herramientas y Técnicas en Gestión de Proyectos PRINCE2 • Plantillas para la Gestión de Proyectos PRINCE2
Título o Certificado	**PRINCE2 FOUNDATIONS**

Fecha de Obtención	FEBRERO 2006
Nombre de la Entidad	**ISACA (Information Systems Audit and Control Association)**
Estudios principales (o campo de trabajo)	• Gobierno de la Seguridad de la Información. Gestión del Riesgo • Gestión del Programa de Seguridad de la Información • Gestión de la Seguridad de la Información • Gestión de Respuestas
Título o Certificado	**CERTIFIED INFORMATION SECURITY MANAGER (CISM).** Titulación acreditada por ANSI (ISO/IEC 17024).

Fecha de Obtención	OCTUBRE 2005
Nombre de la Entidad	**ISACA (Information Systems Audit and Control Association)**
Estudios principales (o campo de trabajo)	• El Proceso de Auditoría de Sistemas de SI. IT Governance • Administración del Ciclo de Vida de Sistemas y de la Infraestructura • Entrega de Servicio y Soporte de TI. Protección de los Activos de Información • Continuidad del Negocio y Recuperación de Desastre

Título o Certificado	**CERTIFIED INFORMATION SYSTEMS AUDITOR (CISA).** Titulación acreditada por ANSI (ISO/IEC 17024).

Fecha de Obtención	JUNIO 2005
Nombre de la Entidad	**EXIN (Examination Institute for Information Science)**
Estudios principales (o campo de trabajo)	• Administración de Incidentes y Service Desk. • Administración de Configuración, Versiones y Cambios. • Administración de Problemas. • Administración de Disponibilidad, Capacidad y Continuidad. • Administración Financiera. Administración de Niveles de Servicios.
Título o Certificado	**ITIL FOUNDATIONS**

Fecha de Obtención	JULIO 2005
Nombre de la Entidad	**APPLUS, Certification Technological Center.**
Estudios principales (o campo de trabajo)	• ISO 17799. • SGSI UNE 71502 / BS7799-2. • Análisis de Riesgos. • Planes de Continuidad.
Título o Certificado	**EXPERTO EN IMPLANTACIÓN DE SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.**

CURSOS SOBRE SEGURIDAD, DEFENSA Y ESPACIO

Fecha (desde – a)	OCTUBRE 2018 – (FECHA ACTUAL)
Nombre de la Universidad, Centro de Formación	EUROPEAN SPACE AGENCY (ESA)
Estudios principales	**CURSOS SOBRE SEGURIDAD, GESTIÓN Y ESPACIO**
Título o Certificado	○ **Acuerdos de propiedad intelectual y licencias.** Este curso cubre los conceptos básicos de la Ley de Propiedad Intelectual, las categorías de acuerdos relevantes, las cláusulas típicas y las trampas en los acuerdos de licencia de software. La formación en informática proporciona una visión general de los derechos de propiedad intelectual y las licencias de software, incluidas las licencias de código abierto. Impartido en el Centro Europeo de Investigación y Tecnología Espacial (ESTEC). ○ **Licencias de código abierto.** Este curso brinda pautas sobre licencias de código abierto (básicas y para oficiales de contratos), una mirada en profundidad a las principales licencias de código abierto, código abierto en el proceso de desarrollo, compatibilidad y cumplimiento de licencias. Cubre explicaciones legales y aspectos prácticos de las licencias de código abierto en general y las licencias de código abierto más comunes. Impartido en el Centro Europeo de Investigación y Tecnología Espacial (ESTEC). ○ **Aprovisionamiento y aspectos contractuales de grandes proyectos de Espacio.** El curso incluye la categoría principal de contratos relevantes para las actividades espaciales (incluidas las diferencias entre I+D y adquisición de satélites), los principales riesgos contractuales y posibles mitigaciones, las diferentes responsabilidades asociadas a los proyectos y los principios de la gestión del cambio contractual. Impartido en el Centro Europeo de Investigación y Tecnología Espacial (ESTEC). ○ **Política del Espacio de la Unión Europea**. Seminario sobre la política espacial de la Unión Europea en el European Space Research and Technology Centre (ESTEC). ○ **Introducción al marco de estándares de la ESA**. Seminario de introducción al marco de estándares de la Agencia Espacial Europea en el European Space Research and Technology Centre (ESTEC). ○ **Gestión de Contratos en la Agencia Espacial Europea**. Seminario sobre el proceso de gestión contractual en la Agencia Espacial Europea en el European Space Research and Technology Centre (ESTEC). ○ **Proceso de revisión técnica de proyectos en la ESA.** Curso sobre el proceso de revisión técnica de proyectos en el European Space Research and Technology Centre (ESTEC).

- **Curso de concienciación sobre Cyber Seguridad por el ESA CERT.** Curso online sobre ciberseguridad impartido por el Centro de Respuesta a Incidentes de la agencia espacial europea (ESA CERT). El curso está formado por 8 sesiones.
- **Procedimientos de continuidad de negocio en la ESA.** El curso incluye 3 seminarios online sobre los procedimientos de gestión de crisis, planes de evacuación y otros temas relacionados con la continuidad del negocio en la Agencia Espacial Europea.
- **Servicios de datos de información clasificada en la ESA.** El curso incluye una descripción general de los servicios y herramientas para la gestión de información clasificada (ERCD) proporcionados por la Agencia Espacial Europea. El curso incluye 4 Módulos: introducción y seguridad física, protección de la información, seguridad personal e incidentes de seguridad.
- **Agile Product Delivery: SCRUM.** El curso cubre la entrega ágil de productos haciendo uso de la Metodología SCRUM, y su aplicación al sector espacial. Curso realizado en el European Space Research and Technology Centre (ESTEC).
- **ESA Knowledge Retention and Transfer Best Practices.** El curso incluye dos seminarios online sobre las mejores prácticas de retención y transferencia del conocimiento en el sector espacial.
- **Space Programs and the Conflict Management Technics.** El curso, realizado en la plataforma online de la Agencia Espacial Europea, trata sobre las técnicas más usadas en la resolución de conflictos en grandes programas del sector espacial.
- **Fraud prevention in the Space Sector.** El curso incluye dos seminarios online sobre las mejores prácticas y los procesos asociados a la hora de prevenir el fraude en grandes programas del sector espacial.

Fecha (desde – a)	MARZO 2015 A JULIO 2018
Nombre de la Universidad, Centro de Formación	NATO Communications and Information Agency (NCIA), NATO Education and Training Facilities, Centros de Excelencia OTAN y otras entidades OTAN.
Estudios principales	**CURSOS SOBRE SEGURIDAD Y DEFENSA**
Título o Certificado	

- **Fundamentos de seguridad de la información**. Introducción al arte y la ciencia de la seguridad de la información en la OTAN. NATO Joint Advanced Distributed Learning System (NATO JADL).
- **Seguridad fronteriza.** Información general y principios del espacio Schengen. NATO Joint Advanced Distributed Learning System (NATO JADL).
- **Seguridad en la era de la información.** Introducción a la naturaleza cambiante de las relaciones internacionales provocada por la revolución de la información, con un enfoque específico en los riesgos y la inseguridad en la era de la información. NATO Joint Advanced Distributed Learning System (NATO JADL).
- **Conocimiento de la defensa cibernética.** Conocimientos básicos y familiarización sobre los temas más importantes y relevantes del área de seguridad informática y seguridad cibernética. NATO Joint Advanced Distributed Learning System (NATO JADL).
- **Curso sobre seguridad de infraestructuras críticas.** Cuestiones de nivel estratégico actual y prospectivo relacionadas con la protección de infraestructuras críticas (CIP). NATO Joint Advanced Distributed Learning System (NATO JADL).
- **Introducción a la protección del medio ambiente en la OTAN**. Introducción a la protección del medio ambiente en un contexto de la OTAN. El curso está dividido en cuatro módulos y está diseñado para ofrecer una visión general de los principales temas de protección ambiental en la OTAN. NATO School Oberammergau.
- **Política de seguridad, relaciones internacionales y tecnología de la información.** Curso que aborda las relaciones entre las políticas / políticas internacionales y las tecnologías de la información modernas. También proporciona un conocimiento básico de herramientas y técnicas de búsqueda en Internet. NATO Joint Advanced Distributed Learning System (NATO JADL).
- **Conciencia sobre la seguridad energética de la OTAN.** El objetivo de este curso es crear conciencia sobre los desarrollos energéticos actuales y proporcionar conocimientos básicos sobre el papel de las nuevas tecnologías para mejorar la eficiencia energética en el ejército y apoyar la protección de las infraestructuras críticas. NATO Energy Security Centre of Excellence.
- **Sistemas de Inteligencia en la OTAN.** El objetivo de este curso es realizar una introducción a los sistemas de inteligencia en la OTAN. NATO School Oberammergau.

- **European Security and Defense Policy (ESDP).** Este curso proporciona una introducción a la Política de Seguridad y Defensa Europea (European Security and Defence Policy – ESDP). NATO School Oberammergau.
- **NATO Civil Emergency Planning - An Overview.** Este curso detalla los roles, orígenes y la organización de CEP (NATO Civil Emergency Planning). Además, el curso describe las herramientas, procesos y procedimientos utilizados por la CEP para llevar a cabo su función. NATO School Oberammergau.
- **Curso de introducción al NATO Energy Security Center.** El objetivo de este curso es familiarizar a los estudiantes con el NATO ENSEC Center of Excellence (COE), su misión, organización, y discutir cómo se proporciona la eficiencia energética en la OTAN, siguiendo las directrices marcadas por el NATO's Chicago Summit. NATO ENSEC Center of Excellence (COE).
- **Introducción a los Satélites de Operaciones.** Este curso se focaliza sobre el comportamiento de los satélites militares. NATO School Oberammergau.
- **NATO JISR Operations Awareness Course.** Este curso proporciona los aspectos clave sobre el proceso de Inteligencia, Vigilancia y Reconocimiento Conjuntos (JSIR - Joint Intelligence, Surveillance and Reconnaissance) en la OTAN. NATO School Oberammergau.
- **Gestión Multinacional de Crisis.** Este curso introduce el concepto de Gestión de Crisis en el entorno OTAN. NATO School Oberammergau.
- **Curso sobre la Infraestructura de Clave Pública en OTAN.** Este curso proporciona una revisión de los conceptos asociados y el funcionamiento de la Infraestructura de Clave Pública (PKI) en OTAN. NATO Communications and Information Systems School.

Fecha (desde – a)	MARZO 2012 A JULIO 2018
Nombre de la Universidad, Centro de Formación	NATO Communications and Information Agency (NCIA), NATO Education and Training Facilities, Centros de Excelencia OTAN y otras entidades OTAN.
Estudios principales	**CURSOS SOBRE TECNOLOGIAS DE LA INFORMACION, EJERCICIOS Y PROCESOS EN EL ENTORNO DE DEFENSA**
Título o Certificado	

- **Recién llegados a la OTAN y conceptos básicos**. Estos dos cursos dan una visión del panorama de la Organización del Tratado del Atlántico Norte. NATO Joint Advanced Distributed Learning System (NATO JADL).
- **Módulo de gestión de ejercicios conjunto.** El módulo de gestión de ejercicios conjuntos (denominada JEMM) es una herramienta de apoyo que respalda la preparación y ejecución de un evento de capacitación en la OTAN. Constituye un depósito central para la documentación de escenarios clave, procesos clave, objetivos de capacitación, líneas maestras, solicitudes de información, observaciones de observadores / entrenadores, etc. NATO Joint Warfare Centre.
- **Operaciones y la era de la información.** Este curso es una introducción a las aplicaciones de TI para respaldar las operaciones militares. NATO Joint Advanced Distributed Learning System (NATO JADL).
- **Curso de Ejercicio asistido por computadora.** Descripción general de la estructura organizativa, las herramientas y los procesos necesarios para llevar a cabo un ejercicio militar asistido por computadora. NATO Joint Warfare Centre.
- **RRT de la OTAN (entrenamiento de expertos).** El módulo de aprendizaje del Equipo de reacción rápida (RRT) está destinado a preparar a los expertos civiles de la OTAN para un posible despliegue fuera de sus lugares de trabajo normales para proporcionar experiencia en nombre de la OTAN. NATO School Oberammergau.
- **Comunicaciones estratégicas de la OTAN.** El objetivo de este curso es familiarizarse con los conceptos básicos de las comunicaciones y el concepto de comunicación estratégica. NATO Strategic Communications Centre of Excellence.
- **Introducción al ETEE de la OTAN - Programación global**. El curso proporciona una comprensión fundamental del enfoque de la OTAN sobre Educación, Capacitación, Ejercicio y Evaluación (ETEE). Describe la estructura de gobierno, la metodología de desarrollo y el proceso de planificación de la producción. NATO Joint Advanced Distributed Learning System (NATO JADL).
- **NATO Lessons Learned Courses.** Dos cursos sobre Lecciones Aprendidas en OTAN, el primero de ellos describiendo la directiva Bi-SC 080-006 por el NATO Joint Analysis & Lessons Learned Center y el Segundo sobre el proceso de Lecciones Aprendidas por el NATO Military Center of Excellence.

- **Curso sobre el proceso de Contratación en la OTAN.** Este curso está compuesto por varios módulos. El objetivo principal del curso es proporcionar una guía detallada sobre el proceso de contratación de la OTAN. NATO School Oberammergau.
- **Cursos sobre Sistemas de Mando y Control Marítimos en OTAN.** Tres cursos sobre los Sistemas de Mando y Control Marítimos en la OTAN, y las entidades que los gestionan. NATO Maritime Interdiction Operational Training Center (NMIOTC).
- **Curso sobre el Joint Warfare Center.** El objetivo de este curso es proporcionar una introducción a las estructuras, funciones y responsabilidades del Centro de Guerra Conjunta (JWC) y a sus misiones operativas actuales. Centro de guerra conjunta OTAN.
- **Curso de planificación de ejercicios en OTAN.** Este curso proporciona una introducción teórica y una descripción general del proceso de planificación del ejercicio conjunto y multinacional de la OTAN. Centro de guerra conjunta de la OTAN.

OTROS CURSOS

Fecha (desde – a)	JUNIO A SEPTIEMBRE 2001
Nombre de la Entidad	ASOCIACIÓN DE TÉCNICOS DE INFORMÁTICA, ATI.
Estudios principales (o campo de trabajo)	• Introducción a la administración de Oracle. Arquitectura de Oracle. • Administración Avanzada. SQLDBA
Título o Certificado	**ADMINISTRACIÓN AVANZADA DE ORACLE**

Fecha (desde – a)	SEPTIEMBRE 1996 A MARZO 1997
Centro de Formación	CEESINE – TISA.
Estudios principales	Instalación y Administración de Equipos y Redes Informáticas.
Título o Certificado	**MÁSTER EN INSTALACIÓN Y ADMINISTRACIÓN DE REDES.**

Fecha (desde – a)	MARZO 1997 A ENERO 2012
Nombre de la Universidad, Centro de Formación	VARIAS INSTITUCIONES: CAJA ESPAÑA, LEGIONET, IDEAL OBJECTS, IONA, ESPELSA, MINISTERIO DE DEFENSA e ISDEFE, etc.
Estudios principales	**CURSOS SOBRE LAS TIC EN VARIAS INSTITUCIONES.**
Título o Certificado	Gestión de Datos en Defensa. Ministerio de Defensa. (20 Horas). Arquitectura y Comunicaciones SAP. (LMDATA, 20 Horas) Servicios de Directorio y Meta directorio. CRITICAL PATH CERTIFICATION. Servicios Web y Arquitectura SOA. ARTIX. (IONA, 20 Horas). Calidad en el Desarrollo del Software (ESPELSA-STC, 100 Horas). Bases de Datos Orientadas a Objetos (Ideal Objects S.A, 25 Horas). Desarrollo Avanzado de Aplicaciones en Internet (ABS, 50 horas). Programación en Java (LEGIONET – CENTRISA, 40 Horas). Arquitectura SIGLO: Cobol CICS DB2, Foundations (CAJA ESPAÑA, 50 Horas) Análisis y Programación Orientada a Objetos (Ideal Objects S.A, 25 Horas). ORBIX y entornos CORBA (Ideal Objects S.A., 20 Horas). Programación en Visual Basic (CSI / CSIF, 200 horas). Diseño Multimedia: Corel Draw y Adobe Premier (CSI / CSIF, 50 Horas.).

IDIOMAS

	ESPAÑOL	INGLES	FRANCÉS
NIVEL	C2	C2	B2

ACTIVIDAD INVESTIGADORA

Más de quince (15) años de experiencia investigadora en diversas universidades y entidades (a tiempo parcial), incluyendo el Departamento de Ingeniería del Software de la Universidad Nacional de Educación a Distancia (UNED), el Departamento de Economía Aplicada VI de la Universidad Complutense de Madrid, y colaborador en proyectos de Investigación y Desarrollo para la Comisión Europea, a través de la empresa pública Isdefe. Se han realizado, dentro de los campos de investigación de auditoría de sistemas, seguridad de la información, bases de datos, modelos económicos de software, economía pública avanzada o análisis del impacto económico, **más de cuarenta (40) artículos** publicados en diversas revistas científicas y técnicas, **más de veinte (20) ponencias** llevadas a cabo en diversos congresos y foros internacionales y **varias publicaciones de libros y capítulos de libros.**

ARTÍCULOS Y PUBLICACIONES

(en orden cronológico)

1. López, J.C.; Heradio, R.; Cerrada, J. A.; J. R. Coz. "***A first-generation software product line for data acquisition systems in astronomy***". SPIE Symposium on Astronomical Telescopes and Instrumentation: Synergies between Ground and Space. Marseille, France, June 23-28, 2008.

This article presents a case study on developing a software product line for data acquisition systems in astronomy based on the Exemplar Driven Development methodology and the Exemplar Flexibilization Language tool. The main strategies to build the software product line are based on the domain commonality and variability, the incremental scope and the use of existing artefacts. It consists of a lean methodology with little impact on the organization, suitable for small projects, which reduces start-up time. SW Product Lines focuses on creating a family of products instead of individual products. This approach has spectacular benefits on reducing the time to market, maintaining the knowledge, reducing the development costs and increasing the quality of new products. The maintenance of the products is also enhanced since all the data acquisition systems share the same product line architecture.

---

2. J. R. Coz; Heradio, R.; Cerrada, J.A.; Lopez, J.C. "***A generative approach to improve the abstraction level to build applications based on the notification of changes in databases***." 10th International Conference on Enterprise Information Systems. Barcelona, Spain, June12–16, 2008.

This paper highlights the benefits, in terms of quality, productivity and time-to-market, of applying a generative approach to increase the abstraction level to build applications based on the notification of changes in databases. Most of the databases maintain meta-tables with information about all stored tables; this information is used in an automatic process to define the software product line (SPL) variability. The remaining variability can be specified by means of domain specific languages. Code generators can automatically query the meta-tables, analyze the input specifications and configure the current product. The paper also introduces the Exemplar Driven Development process to develop code generators and the Exemplar Flexibilization Language that supports the process implementation.

---

3. R. Heradio; J. A. Cerrada; J. C. Lopez; J. R. Coz. *"**Code Generation with the Exemplar Flexibilization Language**"*. Workshop on Generative Technologies (ETAPS'08). Budapest, Hungary, April 5, 2008.

Code Generation is an increasing popular technique for implementing Software Product Lines that produces code from abstract specifications written in Domain Specific Languages (DSLs). This paper proposes to take advantage of the similitude among the products in a domain to generate them by analogy. That is, instead of synthesizing the final code from scratch or transforming the DSL specifications, the final products are obtained by adapting a previously developed domain product.

---

5. J. R. Coz. *"**Estado de madurez de la Seguridad de la Información en las AAPP**". El Blog del Experto de AURIATIC*, Madrid octubre 2010.

Artículo que resume el estado de madurez de la Seguridad de la Información en las Administraciones Públicas.

---

6. J. R. Coz. *"**Impacto de la Gestión de Datos en la Seguridad de la información de las AAPP**". El Blog del Experto de AURIATIC*, Madrid enero 2011.

Artículo que resume el impacto de la Gestión de Datos en la gestión de la seguridad de la información en las Administraciones Públicas.

7. J. R. Coz. *"**Impacto de las certificaciones TIC en la búsqueda de empleo en época de crisis**". Artículo de Opinión en leonnoticias.com.* Abril 2011.
Artículo sobre la importancia de las certificaciones profesionales en la búsqueda de empleo. El artículo expone algunas estadísticas obtenidas de un estudio realizado por el Instituto Innove sobre los portales de búsqueda de empleo en internet y la relación con algunas certificaciones profesionales en materia TIC.

---

8. J. R. Coz, E. Fojón. *"**Panorama Internacional en el establecimiento de Estrategias Nacionales de Ciberseguridad**". Revista SIC. Seguridad, Informática y Comunicaciones.* 06/2011.
Todo estado debe plantearse la necesidad de proteger su Ciberespacio con el objetivo de garantizar su desarrollo social, económico y cultural. Uno de los instrumentos clave para alcanzar este objetivo es la definición de una Estrategia Nacional de Ciberseguridad. En este artículo se enumeran los pilares básicos de las estrategias nacionales de Ciberseguridad existentes en el ámbito internacional y que incluyen el liderazgo desde el Estado, la creación de una estructura organizativa de control, el desarrollo de actividades de formación y concienciación, el impulso económico público - privado, la política exterior, las normalizaciones y regulaciones y, por último, la gestión del I+D+i. Además, se describen algunas estructuras y capacidades desarrolladas por diferentes naciones en el ámbito de la Ciberdefensa.

---

9. J. R. Coz, E. Fojón. *"**Precariedad en la función de auditoría de sistemas en las administraciones públicas**". Revista INNOVATIA.* Junio 2011.
La responsabilidad en el control de los sistemas de información públicos es una función indelegable por parte del Estado. Dentro del paraguas de este control, la función de Auditoria de Sistemas juega un rol muy destacado y las Administraciones Públicas aún no han evolucionado hasta el nivel requerido por los ciudadanos, que demandan unos servicios públicos de calidad, seguros, eficaces y eficientes. Hasta que esta función no se considere estratégica, las administraciones no lograrán la madurez demanda por los ciudadanos. El articulo trata este asunto, describiendo el estado de la función de auditoría en las administraciones públicas.

---

10. J. R. Coz, E. Fojón. *"**La Geoestrategia del Conocimiento en Ciberseguridad**".* Revista RED SEGURIDAD. Madrid. Enero 2012.
El Gobierno de España debe desarrollar una "Geoestrategia del conocimiento en materia de ciberseguridad". Esta estrategia debe disponer del apoyo e implicación de todos los sectores de nuestra sociedad y un compromiso de las fuerzas políticas para que pueda ser mantenido en el tiempo.

---

11. J. R. Coz, E. Fojón C., R. Heradio, J.A. Cerrada. *"**Evaluación de la privacidad de una red social virtual**".* Revista RISTI nº 9, 6-2012. ISSN 1646-9895.
Tanto para las organizaciones y empresas como para la Sociedad en su conjunto, la protección del ciberespacio constituye un aspecto crucial y la privacidad de la información es uno de los pilares sobre los que descansa esta protección. En el proceso de construcción del ciberespacio, las redes sociales virtuales se han convertido en uno de los elementos más relevantes para el intercambio de información, y su utilización de forma global y masiva pone de relevancia su gran importancia estratégica. En este artículo se propone la evaluación de la privacidad en las redes sociales virtuales, mediante un modelo de madurez, un marco para la evaluación y un cuadro integral de mandos.

---

12. J. R. Coz y Vicente Pastor. ***"La conciencia situacional en la Ciberdefensa".*** *Revista SIC (Ciberseguridad, Seguridad de la Información y privacidad).* Febrero 2013.
Una vez que se ha alcanzado suficiente nivel de madurez en las técnicas y medios de ciberdefensa, es necesario continuar mejorando y ser capaces de conocer, dinámicamente, el nivel de seguridad de los sistemas a nuestro cargo para que se posibilite una utilización adecuada de os recursos y la aplicación de los principios de la gestión de riesgos mediante información de las amenazas y modelos probabilísticos obtenidos del análisis de los datos de seguridad. Dado que la situación cambia de manera muy rápida y se requiere una respuesta inmediata a las amenazas de las que se recibe información y a los daños derivados de los incidentes de seguridad, es necesario apoyarse en técnicas de visualización de datos complejos para poder tomar las decisiones adecuadas en el menor tiempo posible. En el presente artículo se expone la situación actual de los sistemas de conciencia situacional para ciberdefensa y se esboza el concepto de visualización de la información como elemento esencial de la conciencia situacional. Por último, se presentan las principales conclusiones.

---

13. J. R. Coz y Vicente Pastor. ***"Retos de la conciencia situacional en la Ciberdefensa".*** *Revista SIC (Ciberseguridad, Seguridad de la Información y privacidad).* Abril 2013.
Aunque está claro que para lograr el control adecuado sobre nuestras infraestructuras TIC es necesario que funcionen nuestros sistemas de conciencia situacional, en muchas ocasiones nos olvidamos de los retos que supone la introducción de nuevas formas de trabajar y nos centramos demasiado en las tecnologías que vamos a adquirir, olvidando prestar una atención adecuada a los procesos que deben ser creados, modificados y adaptados en la empresa y en los cambios organizativos necesarios, que incluyen, en muchas ocasiones, una mejor utilización de los recursos humanos, para integrar esos nuevos sistemas con los existentes en la organización. Se presentan aquí algunos de esos retos junto con recomendaciones de cómo se pueden minimizar los riesgos asociados.

14. J. R. Coz et all. ***"A Domain Engineering Approach to Increase Productivity in the Development of a Service for Changes Notification of the Configuration Management Database".*** *Journal of Software Engineering and Applications. JSEA. Vol.6 No.4, April 2013*. pp. 207-220. DOI: 10.4236/jsea.2013.64026

This paper presents a domain engineering approach to build a software product line that supports the change notification service in a Configuration Management Database (CMDB) according to the Information Technology Infrastructure Library (ITIL) best practices. For the development of this product line, the proposed approach makes use of a construction of products methodology by analogy. This is a new notation, which reports the variability of the products, obtaining metrics as important as the number of products. It uses a language that enables, by means of the flexibilization of a product and the development of some generators, to build the rest of the product line. In addition, the paper offers a standard for the analysis and design of the CMDB as well. Finally, the paper presents an economic model for the product line, where the profitability and productivity of the proposed solution are analysed.

NOTA: Este artículo fue seleccionado por la Revista como uno de los mejores trabajos sobre Ciencia, Comunicaciones e Informática del año 2013.

---

15. J. R. Coz, E Fojón, A. Hernández y G. Colom. ***"Las cibercélulas: una capacidad para la ciberseguridad y la ciberdefensa nacionales".*** *ARI. Real Instituto Elcano. Julio 2013*.

En la actualidad, y salvo países pioneros en la ciberseguridad y ciberdefensa como EEUU, China e Israel, la mayor parte de los países está desarrollando sus capacidades cibernéticas básicas, como sus tecnologías de información y comunicaciones y las organizaciones y procedimientos que las harán funcionar cuando alcancen su madurez. Cuando eso ocurra será necesario articular las organizaciones y procedimientos operativos –cibercélulas– que permitan operar desde esas capacidades previas. Este ARI describe el concepto de las cibercélulas, sus funciones, tareas y ámbitos de actuación, así como los habilitadores que permitirán su funcionamiento. Aunque se trata de una capacidad de siguiente generación y complementaria a las que se están instalando, los autores proponen la necesidad de que se vaya reflexionando en España sobre el tipo de cibercélulas que complementarían las capacidades de ciberseguridad y ciberdefensa que se están instalando para su empleo por las Fuerzas Armadas y las Fuerzas y Cuerpos de Seguridad del Estado.

---

15. J. R. Coz, E Fojón, A. Hernández y G. Colom. ***"Cyber cells: a tool for national cyber security and cyber defense".*** *ARI. Real Instituto Elcano. ARI 26/2013*. Septiembre 2013.

Except for countries that are pioneers in cyber security and cyber defence such as the US, China and Israel, these days most nations are developing basic cybernetic capabilities, such as information and communications technologies and the organizations and procedures that will make them work when they reach maturity. When this happens, it will be necessary to devise the organizations and operational procedures –cyber cells– that allow countries to operate using those previously established capabilities. This paper describes the concept of cyber cells, their functions, tasks and areas of operation, as well as the enablers that will allow them to work. Although it is a matter of a next-generation capability that will complement those which are now being set up, the authors argue that Spain should think about what kind of cyber cells would in fact complement the cyber defence and cyber security capabilities that are being established for use by the military and the national security forces.

---

16. José-Ramón Coz-Fernandez, Rubén Heradio-Gil, José-Antonio Cerrada-Somolinos, ***"Cost Models and Productivity Building Applications Based on the Notification of Changes in Databases".*** *Software Engineering. Vol. 1, No. 2, 2013, pp. 7-12. DOI: 10.11648/j.se.20130102.11*

This paper presents a generative approach to build a Software Product Line (SPL). This SPL is used to build applications based on the Notification of Changes in databases. The paper highlights the benefits, in terms of productivity and cost, using this approach. To obtain the economic data we have used two cost models, the SIMPLE Model (Structured Intuitive Model for Product Line Economics) and one adaptation of COPLIMO (Constructive Product Line Investment Model). Both models demonstrate the great productivity of this SPL.

---

17. José-Ramón Coz-Fernández, Enrique Fojón Chamorro, ***"Modelos y enfoques de ciberseguridad en las redes sociales virtuales".*** Revista RED SEGURIDAD. Madrid. Septiembre 2013.

El ciberespacio evoluciona mediante un proceso de construcción extraordinariamente complejo, y uno de sus elementos más relevantes lo conforman las redes sociales virtuales, que se han convertido en un componente de importancia estratégica. Las redes sociales virtuales facilitan el intercambio de información y su uso masivo tiene un alcance global. En los últimos años el número de ciberataques a este elemento del ciberespacio ha ido en aumento. En este artículo se resumen diversos modelos y enfoques que den soporte a la ciberseguridad las redes sociales virtuales.

---

18. José-Ramón Coz-Fernández.

- ***"Retraso de la Estrategia Nacional de Ciberseguridad".***
- ***"Que nos encontraremos en la nueva estrategia nacional de ciberseguridad".***
- ***"Breve Análisis sobre la nueva Estrategia de Ciberseguridad Nacional".***

Blog de THIBER. Madrid. Septiembre - Diciembre 2013.

Artículos sobre la importancia de la Estrategia Nacional de Ciberseguridad en España y sus ideas clave.

19. José-Ramón Coz-Fernández y otros miembros del Cloud Security Alliance. **Traducción al español de la versión 3d del *Cloud Controls Matrix*, y adaptación de la versión a la LOPD y al ENS.** Cloud Security Alliance, Madrid. Junio 2014.

El Cloud Security Alliance ha publicado una guía que recoge los controles de referencia más importantes en seguridad Cloud, tomando como base los principios publicados en la versión 3 del Cloud Controls Matrix y los requisitos de la normativa española en la materia (Reglamento de la Ley Orgánica de Protección de Datos, RLOPD), y el Esquema Nacional de Seguridad (ENS). Además de la adaptación, se ha traducido de forma completa al español el contenido de los controles. Como resultado, proveedores y clientes disponen en la guía de la referencia nacional más completa para la evaluación de riesgos de seguridad en el ámbito Cloud.

---

20. José-Ramón Coz-Fernández y otros miembros del Grupo de Trabajo de Embajadas de datos de THIBER. **Las embajadas de datos: la protección de la información estatal.** Real Instituto Elcano. ARI 36/2014. Julio 2014.

Estonia está considerando la posibilidad de replicar fuera del país las bases de datos informáticas que permiten la prestación de servicios públicos esenciales para mitigar el daño de una posible agresión o pérdida. La progresiva mentalización de las sociedades y gobiernos frente a los riesgos del ciberespacio les está llevando a dotarse de nuevos instrumentos de ciberseguridad y Ciberdefensa que hace poco parecían de ciencia ficción. El riesgo –ya factible– que corren las bases de datos públicas en el interior de los países está llevando a reforzar sus infraestructuras de tecnologías de la información y las comunicaciones, pero también a pensar en nuevos instrumentos como la replicación de esas bases en el exterior para diversificar los riesgos y potenciar la resiliencia frente a ellos. Este ARI estudia las "embajadas de datos" como opción de respuesta y la forma en la que se podrían articular si se consideran interesantes para la política exterior y la ciberseguridad de un país.

---

21. José-Ramón Coz-Fernández y Vicente Pastor. **Entornos de Sistemas Multiagente y Ciber-Físicos en la Ciberdefensa.** *Revista SIC (Ciberseguridad, Seguridad de la Información y privacidad).* Septiembre 2014.

En el presente artículo se describen las características principales de los sistemas Ciber-inteligentes, denominados MAS&T (Multi-Agent Systems and Technologies), y los sistemas Ciberfísicos, también denominados CPS (Cyber-Physical Systems), y su impacto en el campo de la Ciberdefensa. En los últimos años estos sistemas han cobrado una gran relevancia y en la actualidad son los de mayor potencial en innovación, desarrollo e investigación en este ámbito. Los países más desarrollados han emprendido programas de gran alcance.

---

22. José-Ramón Coz-Fernández. **Francia, un Liderazgo en Ciberdefensa.** *Blog del ISMS Forum Spain.* Octubre 2014.

El artículo describe las características principales que conforman el Liderazgo de Francia en el campo de la Ciberdefensa y los aspectos más relevantes del Programa Nacional de Ciberseguridad dotado con un presupuesto de mil millones de euros y publicado en el año 2014.

---

23. José-Ramón Coz-Fernández y Vicente Pastor. **El reto de la compartición de información en la Ciberdefensa.** *Revista SIC (Ciberseguridad, Seguridad de la Información y privacidad).* Noviembre 2014.

Las inversiones en Ciberdefensa han aumentado casi de forma exponencial en la última década en los países más avanzados, y los presupuestos en grandes programas de ingeniería de TIC de soporte a la Ciberdefensa tienen, en algunos casos, un apoyo presupuestario de varios millones de euros, como es el caso de países en vanguardia, o el caso de organizaciones punteras en Ciberdefensa, como la OTAN. Como consecuencia, los sistemas de soporte a la Ciberdefensa son cada vez más complejos y requieren de arquitecturas interoperables que permitan que el intercambio de información se produzca de forma estandarizada. En esta ocasión, en el presente artículo detallamos algunos de los conceptos, estándares y protocolos con mayor impacto sobre el intercambio de información en la Ciberdefensa a nivel internacional.

---

24. José-Ramón Coz-Fernández. **¡Arabia Saudí, el país del petróleo…y la Ciberseguridad!** *Blog del ISMS Fórum Spain.* Noviembre 2014.

El artículo describe las características principales de las actividades que está llevando a cabo Arabia Saudí en el campo de la Ciberseguridad y los aspectos más relevantes de sus grandes Inversiones en este campo, dotadas con un presupuesto de varios miles de millones de euros.

---

25. José-Ramón Coz-Fernández y otros. **II Edición del Estudio del Estado del Arte de la Seguridad en la Nube.** *Cloud Security Alliance España. ISMS Fórum Spain.* Noviembre 2014.

Durante el año 2014, CSA-ES, iniciativa del ISMS Fórum, ha renovado su visión sobre la seguridad en la Nube en el mercado español e hispanohablante, con la edición 2014 de su Estudio del Estado del Arte de la Seguridad en la Nube. Este estudio ha contado con la información recogida de más de 60 compañías, principalmente basadas en España y también de otras geografías, en particular en el continente americano.

---

26. José-Ramón Coz-Fernández. **¡El Ciber Reino Unido, una gran apuesta por la Ciberseguridad y la Ciberdefensa!** *Blog del ISMS Forum Spain.* Enero 2015.
El artículo describe las actividades de tipo estratégico y los programas que está desarrollando el Reino Unido en el campo de la Ciberseguridad y la Ciberdefensa, dotados con un presupuesto de más de 1.000 M€.

---

27. José-Ramón Coz-Fernández y Vicente Pastor. **STIX: ¿el estándar para la compartición de la información de la ciberdefensa?** *Revista SIC (Ciberseguridad, Seguridad de la Información y privacidad).* Febrero 2015.
En el presente artículo se concluye el análisis de alto nivel sobre la compartición de la información en Ciberdefensa que ya iniciaron los autores en la edición de SIC de noviembre de 2014, donde en el artículo denominado "*El reto de la compartición de información en la Ciberdefensa*" detallaron algunos de los conceptos, estándares y protocolos con mayor impacto sobre el intercambio de información en la Ciberdefensa a nivel internacional. En esta entrega profundizan en una de las propuestas existentes que facilitan la automatización de este proceso, al respecto de la cual ofrecen algunos apuntes de por qué creen que es la que tiene más posibilidades de convertirse en el estándar de facto para comunicar amenazas, incidentes y otros observables, que permitirán a otras organizaciones defenderse de los ataques ya sufridos por una organización. Estamos hablando de STIX (Expresión estructurada de información sobre amenazas), una iniciativa de la corporación estadounidense MITRE para describir inteligencia sobre Ciberamenazas.

---

28. J. R. Coz. *"**Los perfiles de Ciberseguridad, bajo demanda**". Revista INNOVATIA.* 02/2015.
El crecimiento del mercado de la Ciberseguridad en los países más avanzados tecnológicamente está suponiendo un cambio en los procesos de incorporación del personal con experiencia y conocimientos en este campo. La gran demanda en muchos casos es muy superior a la oferta y el gran dinamismo del propio sector está llevando a realizar planes educativos y de formación que incorporen estos aspectos, como ya está sucediendo en multitud de países con una enorme inversión como los Estados Unidos, Francia, Rusia, Israel, Arabia Saudí o el Reino Unido. El artículo expone algunos conceptos sobre la ciberseguridad y analiza la importancia de la formación profesional en este campo.

---

29. J. R. Coz, E. Fojón. *"**Las diferentes velocidades de la ciberdefensa en el ámbito de la OTAN**". THIBER - El Mundo.* Marzo 2015.
Breve artículo sobre la necesidad de que todos los aliados desarrollen cibercapacidades específicas porque difícilmente podrán valerse de los medios propios de la OTAN o aprovecharse de las capacidades del resto de los miembros, muchos de los cuales son reticentes a exponer sus ciberfuerzas.

---

30. J. R. Coz, V. Pastor. *"**Sin coordinación efectiva no hay Ciberdefensa**". CIBER – Real Instituto Elcano. Abril* 2015.
Este artículo pretende mostrar las organizaciones e iniciativas de coordinación que existen en otros países para facilitar la compartición de la información y contribuir a la defensa colectiva del ciberespacio en materia de prevención y respuesta a incidentes de seguridad.

---

31. José-Ramón Coz-Fernández y Vicente Pastor. **ISAC como nexo de unión de las arquitecturas en Ciberdefensa.** *Revista SIC (Ciberseguridad, Seguridad de la Información y privacidad).* Abril 2015.
En el campo de la Ciberdefensa una de las estructuras más relevantes lo constituyen los Centros de Compartición y Análisis de Información, o en sus más conocidas siglas ISAC (Information Sharing and Analysis Center). En el presente artículo describimos las características principales de estos centros y su impacto en la Ciberdefensa.

---

32. José-Ramón Coz-Fernández. **Los Cibercomandos y la Segregación de Funciones.** *CIBER – Real Instituto Elcano. Junio* 2015.
El articulo trata sobre los Cibercomandos y la Segregación de Funciones. También se analiza como este aspecto puede ser abordado con Controles Compensatorios y Auditorias, tal y como se lleva a cabo en los Programas de Ciberdefensa más relevantes a nivel internacional.

---

33. José-Ramón Coz-Fernández y Vicente Pastor. **La Ciberdefensa militar ante el reto de Internet de las Cosas.** *Revista SIC (Ciberseguridad, Seguridad de la Información y privacidad).* Abril 2015.
La práctica totalidad de los elementos de soporte a la Ciberdefensa en las organizaciones y empresas con un alto grado de madurez a nivel internacional precisarán, a corto plazo, de diversos cambios de gran relevancia. ¿Cuál es el disparador de estos cambios? Se trata del aspecto que está añadiendo una mayor complejidad en el entorno de la Ciberdefensa, si cabe, y es la consideración de la interconexión múltiple a la red de una gran variedad de dispositivos físicos. Este concepto, que los especialistas en Ciberdefensa comienzan a analizar bajo el paraguas de la arquitectura de sistemas, se conoce como Internet de las Cosas (IoT), y presenta una serie de nuevos retos que deben ser abordados con gran premura.

---

34. J. R. Coz, V. Pastor. *"**No sé lo que pasa en mi red. ¿Puedo protegerla adecuadamente?**". CIBER – Real Instituto Elcano.* Octubre 2015.
Este artículo pretende mostrar las dificultades que se presentan para ejercer una ciberdefensa eficaz el hecho de que los procesos, las tecnologías y los equipos humanos que se dedican a la gestión de los sistemas de información y los que se dedican a defenderlos de ataques externos, estén separados unos de otros.

---

35. J. R. Coz, E. Fojón. *"**Ciberseguridad nacional, una necesidad**". El español.* Noviembre 2015.
Este artículo resume los principales pasos a abordar previos al diseño de un gran programa de ciberseguridad nacional, en línea con lo llevado a cabo en los países más desarrollados en este campo y la situación de madurez de la ciberseguridad nacional.

36. José-Ramón Coz-Fernández y Vicente Pastor. **Nuevo espacio de educación superior en Ciberdefensa en el ámbito internacional.** *Revista SIC (Ciberseguridad, Seguridad de la Información y privacidad).* Junio 2016.
En el presente artículo se describen las características principales del espacio de educación superior en el ámbito de la ciberseguridad a nivel internacional, destacando las principales disciplinas que cubre y la situación respecto a las titulaciones ofrecidas en otros países. En los últimos años, la demanda de profesionales en este campo, principalmente en los países más desarrollados y con una clara apuesta por la tecnología y la seguridad, ha crecido de tal forma que los sistemas educativos no han respondido en muchas ocasiones con la premura mostrada por la industria y, en general, el mercado. En la actualidad, la evolución es muy importante y existe un conjunto de disciplinas de carácter general que son cubiertas por los espacios educativos de nivel superior y ya se han consolidado algunos másteres y grados que están teniendo una gran acogida por el mercado y la administración.

---

37. J. R. Coz, V. Pastor. *"**La incubadora de proyectos de ciberseguridad de la OTAN y otras iniciativas internacionales**". CIBER – Real Instituto Elcano.* Septiembre 2016.
En el presente artículo describimos brevemente las características principales de una de las iniciativas más importantes de la OTAN en ciberseguridad. Se trata de la incubadora de proyectos encuadrada dentro de los esfuerzos que está realizando la Organización en su asociación con la industria y el entorno académico para los temas relacionados con la ciberseguridad (NICP – NATO-Industry Cyber Partnership). En los últimos años se han puesto en marcha una serie de iniciativas en este campo que han cobrado una gran relevancia y en la actualidad constituyen los pilares de la innovación e investigación en ciberseguridad dentro de la OTAN. De manera similar, los países más desarrollados en este campo y diversas organizaciones internacionales están llevando a cabo programas y proyectos de gran alcance que conllevan el desarrollo de iniciativas similares. Por su grado de ambición destacamos en este artículo esta iniciativa, aunque también explicamos brevemente algunos de los esfuerzos multinacionales más destacados.

---

38. J. R. Coz. *"**El papel de la ciberseguridad en la gestión comunicativa en las organizaciones**". Revista INNOVATIA n. 55.* Madrid, marzo 2018.
En el mencionado artículo publicado en la revista INNOVATIA, se describe el papel de la ciberseguridad dentro de la gestión comunicativa, y como los diferentes aspectos que cubre la ciberseguridad pueden dar apoyo a los retos a los que se enfrenta la comunicación en todas las organizaciones. La principal conclusión del artículo es que las características principales de los procesos de comunicación organizativa deben estar soportadas por una adecuada ciberseguridad.

---

39. J. R. Coz, A Valiño Castro, S. Acosta Ortega. *"**El impacto económico de la Armada en la economía española en 2017**". Revista General de Marina. ISSN: 0034-9569.* Julio 2019.
En el mencionado artículo se analiza en detalle el impacto de la actividad económica de la Armada sobre la economía nacional en el 2017, incluyendo el incremento generado en la producción, la renta y el empleo. Para el análisis se ha utilizado el modelo de gestión del conocimiento económico MOCIE, que permite medir el impacto económico de los programas sobre la economía nacional. URL de la revista:
http://www.armada.mde.es/archivo/rgm/2019/07/RGM%20Julio%202019%20V%20FINAL%20IMPRENTA.pdf
URL del artículo: http://www.armada.mde.es/archivo/rgm/2019/07/rgm072019cap07.pdf

---

40. J. R. Coz, A Valiño Castro. *"**Integración de un modelo de gestión del conocimiento para evaluar el impacto económico en la gestión de programas del sector de la defensa**". Revista de Economía Industrial Núm.412: Industria de Defensa.* Páginas 57 – 65. Septiembre 2019.
En el presente artículo se pretende analizar los aspectos centrados en el control de los programas de Defensa. Se abordan las características principales del marco de control de los programas de defensa, destacando los principales estándares, guías, y buenas prácticas. El modelo del conocimiento para el impacto económico, denominado MOCIE, junto con el sistema de información de soporte a este modelo, se presentan igualmente y se describe como el modelo MOCIE puede ser integrado dentro del marco de la gestión de programas en el ámbito de la defensa. Se presentan conclusiones y algunos trabajos futuros.
URL de la revista: https://www.mincotur.gob.es/es-ES/servicios/Documentacion/Publicaciones/Paginas/detallePublicacionPeriodica.aspx?numRev=412
URL del artículo completo:
https://www.mincotur.gob.es/Publicaciones/Publicacionesperiodicas/EconomiaIndustrial/RevistaEconomiaIndustrial/412/COZ%20FERNÁNDEZ%20y%20VALIÑO%20CASTRO.pdf

41. J. R. Coz, and Vicente Pastor. *"**The complexity of performing cyber audits in the space sector along the supply chain".** Cyber Security: A Peer-Reviewed Journal. Volume 4. November 2020.*
Las auditorías cibernéticas no son nada fáciles de realizar. El número de dependencias presentes en los sistemas modernos hace que el proceso y los hallazgos, cuando están disponibles, son difíciles de interpretar y comprender. La creciente tendencia a subcontratar grandes partes de un programa o proyecto esconde algunas de esas dependencias y otros detalles bajo una gran cantidad de contratos y otra documentación legal que, en algunos casos, obliga al auditor a convertirse en un verdadero arqueólogo en búsqueda del Santo Grial. En este artículo, los autores introducen el concepto de auditorías cibernéticas, explican algunos de los factores que influyen en la complejidad de los proyectos en el sector espacial a lo largo de la cadena de suministro y describen herramientas que pueden facilitar el proceso de auditorías cibernéticas. URL: https://www.henrystewartpublications.com/csj/v4

---

42. J. R. Coz. *"**Auditing IT Governance in the Navigation Sector".** ISACA Journal, news and trends. 29 Marzo de 2021.*
Auditar la gobernanza de TI en el sector de la navegación es un desafío. La cantidad de interdependencias en los nuevos sistemas de navegación hace que el proceso sea realmente complejo. Es importante comprender el concepto de auditorías cibernéticas en el sector de la navegación, identificar algunos de los factores que contribuyen a la complejidad de los proyectos en el sector de la navegación a lo largo de la cadena de suministro y reconocer cómo COBIT® puede contribuir a los diferentes análisis realizados. URL de la revista: https://www.isaca.org/resources/news-and-trends/industry-news/2021/auditing-it-governance-in-the-navigation-sector

---

43. J. R. Coz, A Valiño Castro. *" **El impacto industrial y económico de los programas espaciales en Europa en el post-COVID-19: sus implicaciones en la política industrial"**. Revista de Economía Industrial Núm.420: Geoeconomía Industrial.* Páginas 67 – 80. Septiembre 2021.
En el artículo se analizan inicialmente las características del sector y de la industria espacial en el mundo, poniendo en su lugar la industria espacial europea y española. Se analiza la política espacial europea y se pone énfasis en las implicaciones de los nuevos Programas del Espacio propuestos por la Unión Europea y Agencia Espacial Europea (ESA), analizando el impacto de estos programas sobre la industria espacial y la Política Industrial española. URL de la revista:
https://www.mincotur.gob.es/es-ES/Publicaciones/Paginas/detallePublicacionPeriodica.aspx?numRev=420
URL del artículo completo:
https://www.mincotur.gob.es/Publicaciones/Publicacionesperiodicas/EconomiaIndustrial/RevistaEconomiaIndustrial/420/Coz%20Ferna%CC%81ndez%20y%20Valin%CC%83o%20Castro.pdf

---

44. J. R. Coz, A Valiño Castro. *"**Las nuevas capacidades estratégicas para la Unión Europea proporcionadas por el sector espacial. Especial referencia a las PNT**". Revista de Economía Industrial Núm.430: Industria de Defensa.* Páginas 65 – 72. Marzo 2024.
La actuación de la UE en el espacio se lleva a cabo a través de la Agencia Espacial Europea con la colaboración de los países integrantes. Esta colaboración se ha visto favorecida por el elevado coste de los proyectos aeroespaciales y ha originado una experiencia considerable en la realización de proyectos conjuntos en el sector aeroespacial militar y civil que, dadas las amenazas, están totalmente imbricados en este sector. En el artículo analizamos las capacidades estratégicas proporcionadas por la política espacial, con una especial referencia a las de posicionamiento, navegación y temporización, y su importancia en el desarrollo industrial. URL de la revista:
https://www.mintur.gob.es/es-ES/Publicaciones/Paginas/detallePublicacionPeriodica.aspx?numRev=430
URL del artículo completo:
https://www.mintur.gob.es/Publicaciones/Publicacionesperiodicas/EconomiaIndustrial/RevistaEconomiaIndustrial/430/COZ%20FERN%C3%81NDEZ%20Y%20VALINO.pdf

---

45. J.R.C. Fernández and R.B. Hijón, ***"Cybersecurity Audits of the Supply Chain within the Galileo Ground Control Segment"**. Trans. Appl. Sci. Eng. Technol., vol. 1, no. 1, pp. 1-9, 2025.*
Auditing the compliance of cybersecurity processes, regulations, requirements, and policies in the navigation sector is a real challenge. The number of interdependencies and the stakeholders in the new navigation systems make the processes truly complex, and the increasing trend in subcontracting big parts of a system hides some of those interdependencies and other details in a huge number of assets and other regulatory and legal documentation obliges the auditors to become archaeologists to assess the cybersecurity status. In this article, the authors introduce the experience of cybersecurity audits in the navigation sector within the ground control segment (GCS) and explain some of the factors that contribute to the complexity of this activity.
URL del Paper:
https://lanashscience.com/article/cybersecurity-audits-of-the-supply-chain-within-the-galileo-ground-control-segment .
URL del artículo completo: https://lanashscience.com/articles_file/127-_article1740994400.pdf

---

PONENCIAS EN CONFERENCIAS Y CONGRESOS

(en orden cronológico)

1. J. R. Coz; R. Heradio; J. A. Cerrada; ***"Construcción de una Línea de Productos, utilizando la tecnología de Gestión de Colas, mediante un enfoque generativo"***. Congreso XVIII Nacional de Usuarios Oracle. Málaga, octubre 2008.

La ponencia versa sobre la presentación de un Framework que se ha diseñado para la construcción de aplicaciones basadas en los mecanismos de notificación de cambios de Oracle. El Framework a presentar se utiliza para la construcción líneas de productos software (SPL) utilizando un enfoque basado en la programación generativa.

---

2. J. R. Coz "***Uso de las Buenas prácticas de Gestión ofrecidas por PRINCE2 aplicadas en la Gestión Funcional de Registros Judiciales***". 3ª Edición del Foro Internacional de Gestión de Proyectos PRINCE2, Madrid, junio 2009.

Ponencia resumen sobre el proyecto de aplicación de las buenas prácticas PRINCE2 en la Subdirección de Registros Judiciales del Ministerio de Justicia para la gestión de cambios funcionales en grandes sistemas.

---

3. A. Sanz Villalba, J. R. Coz. ***"Migración a PRINCE2 desde una metodología de Gestión de Proyectos ad hoc en entornos de alta seguridad"***. 4ª Edición del Foro Internacional de Gestión de Proyectos PRINCE2, Madrid, junio 2010.

Ponencia sobre el uso de las buenas prácticas de Gestión de Proyectos aplicadas a sistemas en el entorno de la Defensa.

---

4. J. R. Coz, E. Fojón C., R. Heradio, J.A. Cerrada. ***"Cuadro Integral de Mandos como soporte al proceso de Evaluación de la Madurez de una Red Social Virtual en materia de Privacidad "***. ITGSM'2010. V International Congress on IT Governance and Service Management: Proposals for Tough Economic Times. Alcalá de Henares, junio 2010.

En los últimos años las Redes Sociales Virtuales se han convertido en uno de los servicios más populares para el intercambio de información, mayoritariamente de carácter personal, y su uso global pone en relevancia su importancia. En este artículo se resume el Modelo de Madurez en Materia de Privacidad para una Red Social Virtual, el Framework de Evaluación de la Madurez y, además, se detalla una Herramienta de Apoyo a la Evaluación, en forma de Cuadro Integral de Mandos.

---

5. J. R. Coz, E. Fojón. ***Un modelo educativo para una Estrategia Nacional de Ciberseguridad***. Congreso ENISE (Encuentro Internacional de la Seguridad de la Información). León. Octubre 2011.

Proporcionar garantías razonables para un adecuado desarrollo cultural, social y económico en un país es una responsabilidad indelegable del Estado. Dentro del amplio abanico de esta responsabilidad, la función de protección de la Ciberseguridad desempeña un rol muy destacado. Uno de los instrumentos clave utilizados por los países de nuestro entorno es la definición de una Estrategia Nacional de Ciberseguridad. Las estrategias internacionales puestas en marcha basan su funcionamiento en una serie de pilares básicos. Un pilar muy destacado es la Educación. Este artículo resume las características más relevantes de la educación en esta materia y propone un modelo para su gestión.

---

6. J. R. Coz, E. Fojón y otros. ***"La ciberseguridad. Consideraciones estratégicas y Modelos de Referencia en el ámbito internacional"***. I Foro de Ciberseguridad del Spanish Cyber Security Institute. 20.11.2012. Madrid

En esta breve ponencia se presentan algunas consideraciones estratégicas sobre la Ciberseguridad y posteriormente se analizan esas consideraciones estratégicas desde un punto de vista práctico, exponiendo algunos modelos de referencia en el ámbito internacional.

---

7. J. R. Coz y otros. ***"Estudio del Estado de la Seguridad en el Cloud Computing en España".*** *Jornada Internacional de Seguridad de la Información del ISMS Fórum. Madrid, Auditorio Mutua Madrileña, 20 de Noviembre de 2014.*

La ponencia resume las principales conclusiones sobre el estado de la seguridad en el Cloud Computing en España en el año 2014, incluyendo aspectos como el grado de uso de la nube, los servicios más demandados, las expectativas de Seguridad, los requisitos técnicos de seguridad, la satisfacción de los Usuarios de Nube, los modelos de servicio y los incidentes de seguridad. Documento: URL . URL de la Jornada: URL

---

8. J. R. Coz, R. Delgado, M. Rodríguez y T. Arroyo. ***"Herramienta de Autoevaluación de la Madurez en Gobierno TI basada en COBIT-PAM"***. *Comisiones de Trabajo ISACA.* 10.09.2015. Madrid

En esta conferencia se presenta una herramienta que permite autoevaluar la madurez de una organización en Gobierno Ti basada en el proceso COBIT-PAM.

9. J. R. Coz. *"**Modelo de gestión del conocimiento económico basado en el marco input output. Un caso de estudio aplicado al sector de la defensa en España"**. II Congreso Internacional de Estudios Militares. CIdEM 2016. Granada, 18-20 de octubre 2016.*
En esta conferencia se presenta el modelo de gestión del conocimiento económico MOCIE que permite medir el impacto económico de los programas del sector de la defensa en España y se presentan las principales conclusiones de un caso de estudio.

---

10. J. R. Coz. *"**La gestión del conocimiento y el impacto económico en la nueva economía de la Defensa. Un caso de estudio: el mantenimiento de aeronaves"**. Jornadas Aeroespaciales de Economía de la Defensa del Ejército del Aire. Madrid. Marzo 2017.*
En estas jornadas se presentó un proyecto de investigación emblemático y novedoso que puede aportar una mejora notable en la gestión económica de los programas de defensa, se analizó el contexto económico de la Defensa y se aportaron las principales conclusiones de este proyecto y sus lecciones aprendidas. Durante el proyecto de investigación se ha desarrollado un caso de estudio de gran alcance dentro del Sector de la Aeronáutica de la Defensa: el mantenimiento de aeronaves.

---

11. V. Pastor y J. R. Coz. *"**¿Por qué es tan difícil caracterizar el ciberespacio? Aproximaciones válidas para la Ciberdefensa"**. III Congreso Internacional de Estudios Militares. CIdEM 2018. Granada, 18-20 de octubre 2018.*
Esta comunicación describe algunas de las dificultades relacionadas con la gestión del conocimiento y la maniobrabilidad en el ciberespacio, y algunas aproximaciones útiles que permitan obtener información relevante que dé soporte a las operaciones.

---

12. J. R. Coz. *"**Retos de Ciberseguridad en entornos Críticos. El segmento terreno de Galileo"**. XXX Congreso Global de Ciberseguridad, Seguridad de la Información y Privacidad, SECURMATICA. Madrid, 23-25 de abril 2019.*
En esta ponencia se describen algunos de los principales retos de la ciberseguridad en entornos críticos. La ponencia describe como caso de uso el segmento terreno del Programa europeo de navegación por satélite Galileo, un programa con un presupuesto de más de 1.500 millones de euros.
URL de las conferencias: https://securmatica.com/pdf/2019-programa7.pdf

---

13. J. R. Coz. *"**The Big Challenges to Perform a Cyber Audit. The Case of Galileo Program"**. EuroCACS/CSX Conference. Ginebra, Suiza, 16-18 de Octubre de 2019.*
En esta ponencia se describen algunos de los principales desafíos a la hora de realizar una auditoria cibernética de un programa complejo. La ponencia describe como caso de uso el Programa europeo de navegación por satélite Galileo, un programa con un presupuesto de más de 1.000 millones de euros anuales.
URL de las conferencias: https://next.isaca.org/conferences/euro-cacs-csx-2019

---

14. J. R. Coz. *"**Planning Complex Cyber Audits. The Case of Galileo Ground Segment"**. Infosecurity ISACA North America Expo and Conference. Nueva York, USA, 18-20 Noviembre de 2019.*
En esta ponencia se describen las principales actividades y problemas a los que se enfrentan los auditores a la hora de planificar auditorias cibernéticas complejas en grandes programas con un gran impacto político y económico. La ponencia describe como caso de uso el segmento terreno del Programa europeo de navegación por satélite Galileo, un programa con un presupuesto de más de 1.500 millones de euros.
URL de la conferencia: https://www.infosecuritynorthamerica.com/en/Sessions/80849/Planning-Complex-Cyber-Audits-The-Case-of-Galileo-Ground-Segment-1500-MEuros

---

15. J. R. Coz. *"**Lecciones aprendidas sobre planificación de auditorías en entornos internacionales**" Congreso de ISACA Iberoamérica 2020. 26-30 de Octubre de 2020.*
En el congreso "*ISACA Iberoamérica 2020, ciberseguridad, un desafío que trasciende fronteras*", organizado con la colaboración de más de veinte capítulos de la ISACA a nivel internacional, y difundido online, se presentaron dos ponencias sobre las principales lecciones aprendidas durante el desarrollo de la preplanificación y la planificación de las ciber auditorias en entornos internacionales, con despliegues logísticos complejos.
Enlace a la primera conferencia:
https://www.brighttalk.com/webcast/18299/446003?utm_source=Reed+Exhibitions&utm_medium=brighttalk&utm_campaign=446003
Enlace a la segunda conferencia:
https://www.brighttalk.com/webcast/18299/451175?utm_source=Reed+Exhibitions&utm_medium=brighttalk&utm_campaign=451175

---

16. J. R. Coz. *"**Planning complex cybersecurity audits in the space sector".** V-Applied2021 3rd Edition of Applied Science, Engineering and Technology Webinar, 27-28 March, 2021, Live Stream.*
The cybersecurity audits are described as the evaluation of the level of compliance of the information security management system and implemented security measures with defined requirements, security policies in place and the appropriate safety standards. The conference described the main challenges to plan these cybersecurity audits, and the most relevant lessons learnt at the European Space Agency.
URL de la conferencia: https://www.sciwideonline.com/appliedscience-virtual

---

17. J. R. Coz. *"**La logística en la planificación de auditorías en el sector espacial".*** ISACA Madrid Event 2021. Sesion 1. 3 de Junio de 2021 (Online).
La ponencia trata sobre el problema de la planificación logística en las ciber auditorias del sector espacial. En la conferencia se exponen el proceso de Ciberauditorias del sector de la navegación en la Agencia Espacial Europea, los principales elementos a considerar durante la planificación y cómo la logística impacta en las diferentes actividades que se llevan a cabo durante la ejecución de las ciber-auditorias.

---

18. J. R. Coz. *"**The importance of the Logistics within the Cybersecurity Audits in the Navigation Sector".** V-Applied2022. 3rd Global Webinar on Applied Science, Engineering and Technology. V-Applied2022. Theme: Contemporary Challenges and Practical Solutions in Applied Science and Engineering. Febrero de 2022.*
La ponencia trata sobre el proceso de logística durante la planificación de las ciber auditorias del sector espacial de la Navegación. En la conferencia se exponen los principales elementos a considerar durante la planificación logística y cómo impacta el proceso logístico en las diferentes actividades que se llevan a cabo durante la ejecución de las ciber-auditorias y en la cadena de suministro asociada.
URL de la conferencia: https://www.globalscientificguild.com/3rd-applied-science/

---

19. J. R. Coz. *"**Lecciones aprendidas planificando auditorias en la Agencia Espacial Europea".** Evento C-Meet sobre Digitalización e Innovación. Santander, Septiembre de 2022.*
En la ponencia se exponen las principales lecciones aprendidas, recopiladas durante cuatro años, a la hora de planificar de auditorías de Ciberseguridad en la Agencia Espacial Europea. Además, la ponencia presenta las peculiaridades del sector espacial y como la complejidad de su cadena de suministro impacta durante el proceso de auditoría y los principales aspectos a considerar, incluyendo herramientas, recursos humanos, procedimientos y técnicas.
URL de la Conferencia: https://c-meet.es/c-meet-ciberseguridad-digitalizacion-innovacion/
Presentación: https://www.youtube.com/watch?v=awpbjH6x-YQ
Conferencia: https://www.youtube.com/watch?v=kLw1w_HX82I&t=23720s
Entrevista: https://www.youtube.com/watch?v=M_SspKk_dbo

---

20. J. R. Coz. *"**La ESA, el sector de la navegación y las oportunidades de empleo".** Evento **organizado por la Universidad Europea del Atlántico** (URL) Santander, Mayo de 2023.*
En la ponencia se exponen los principales programas dirigidos por la Agencia Espacial Europea, con especial énfasis en los programas del sector de la Navegación, y las diferentes oportunidades de empleo que ofrece el sector. La ponencia forma parte de una serie de jornadas sobre empleo organizadas por la Universidad Europea del Atlántico. URL

---

21. J. R. Coz. *"**Experiencia de la Agencia Espacial Europea con las auditorias de ciberseguridad en el sector de la navegación.** XXV Jornada Internacional de Seguridad de la Información del ISMS Fórum. Madrid, Cívitas Metropolitano, 16 de Noviembre de 2023.*
La ponencia resume los principales aspectos de las auditorias de ciberseguridad coordinadas desde la Agencia Espacial Europea en el sector de la navegación. Anualmente se coordinan casi un centenar de auditorías sobre toda la cadena de suministro, distribuida por todo el mundo, que proporciona servicios y productos relacionados con los servicios de posicionamiento, navegación y tiempo. URL

---

22. J. R. Coz. *"**Experiencia de la Agencia Espacial Europea con las auditorías de ciberseguridad. La protección de una inversión de más de 6 billones de euros en sistemas de navegación".** Conferencia Internacional ENISE número 18. León. Octubre de 2024.*
En la jornada se pusieron de manifiesto los aspectos más críticos de las auditorías de ciberseguridad realizadas por la industria espacial, y coordinadas por la Agencia Espacial Europea dentro de los programas de la Unión Europea relacionados con el sector PNT (Posicionamiento, Navegación y Tiempos). En la actualidad, el PNT es el mayor sector económico del sector espacial, y el presupuesto cubierto supera los *6.000 millones de euros*.
URL de la conferencia: URL. Evento completo: DIA 1, DIA 2
Conferencia: https://youtu.be/jVycW4a_Vec?t=22485

23. J. R. Coz. *"**European Space Agency experience with Cybersecurity Audits for PNT. The critical aspects of the Cyber Internal Audits**". Charlas organizadas por la Agencia Europea del Medicamento. Ámsterdam, Países Bajos. 25 de Octubre de 2024.*
La charla se realizó en el contexto de las sesiones organizadas por la Agencia Europea del Medicamento, que reúne a Auditores Internos de diversas agencias europeas como la ESA, EUROPOL, F4E, EIB, EASA, EPO y otros. En la charla se resumen los principales retos que afrontan las auditorías internas, y se reflexiona sobre la complejidad en el caso del sector espacial y los sistemas de navegación.

LIBROS Y CAPÍTULOS DE LIBROS

(en orden cronológico inverso)

1. Auditando Sistemas Industriales e Infraestructuras Críticas. Cuadernos ISACA, Capítulo de Madrid. Noviembre 2020.
Este documento tiene como objetivo presentar y describir un modelo para auditar sistemas de control industriales y de infraestructuras críticas, mostrando la metodología que se debe seguir con la revisión del análisis de riesgos, de los modelos de control y de las pruebas periódicas que se deben hacer para su verificación, con objeto de concluir sobre la madurez del entorno.
http://www.isaca.org/chapters7/Madrid/members/Pages/Publicaciones.aspx

2. Identificación y Control de Riesgos en Procesos Validados con Blockchain. Cuadernos ISACA, Capítulo de Madrid. Noviembre 2020.
Este documento, elaborado por un grupo de expertos del Capítulo de Madrid de ISACA, profundiza sobre los diferentes controles y riesgos asociados a los procesos que hacen uso de la tecnología de Blockchain y su impacto en la ciberseguridad.
http://www.isaca.org/chapters7/Madrid/members/Pages/Publicaciones.aspx

3. Auditoría cumplimiento sobre Sistemas en la Nube. Cuadernos ISACA, Capítulo de Madrid. Noviembre 2020.
El objetivo de este documento es definir una guía que oriente y ayude a los Auditores a organizar y realizar una auditoría de entornos de Nube. Para ello, se presentarán unas bases sobre qué es la Nube, cómo se realiza el aseguramiento de sistemas en la Nube y cuáles son los factores a tener en cuenta sobre la auditoría de la Nube. Dando además una guía práctica con algunos de los puntos que se han considerado más representativos para la realización de una auditoría de servicios en la Nube.
http://www.isaca.org/chapters7/Madrid/members/Pages/Publicaciones.aspx

4. Seguridad y Defensa. Estrategias y desafíos de un mundo globalizado. Volumen I, Parte II, sobre la caracterización del Ciberespacio. ISBN: 978-84-338-6520-5. Páginas 341-365. Universidad de Granada. 2019.
Esta obra ha sido consolidada tras el Congreso de Estudios Militares celebrado en la Universidad de Granada en Octubre de 2018, en el marco de un Convenio de Colaboración entre la Universidad de Granada y el Ministerio de Defensa, que durante más de 25 años ha conseguido aunar Universidad y Ejército en actividades de formación e investigación. La parte II de la obra trata, entre otros aspectos, un capítulo sobre la dificultad de caracterizar el Ciberespacio.
http://cemixugrmadoc.ugr.es/pages/7-publicaciones/7a-biblioteca-conde-de-tendilla-directorio/28seguridadydefensa/

5. Nuevos Modelos de Análisis de Riesgos en Ciberseguridad. Cuadernos ISACA, Capítulo de Madrid. Noviembre 2018.
Este documento, elaborado por un grupo de expertos del Capítulo de Madrid de ISACA, analiza la situación a la que se enfrentan las organizaciones cuando tienen que gestionar riesgos asociados a la Ciberseguridad. Como resultado del análisis se propone un modelo de análisis de riesgos dinámico específico para la Ciberseguridad.
http://www.isaca.org/chapters7/Madrid/members/Pages/Publicaciones.aspx

6. Revisando la función de Auditoria de Sistemas en la empresa digitalizada. Cuadernos ISACA, Capítulo de Madrid. Noviembre 2018.
Este documento, elaborado por un grupo de expertos del Capítulo de Madrid de ISACA, revisa la función de auditoria de sistemas dentro de la empresa. Esta función tiene como objetivo principal garantizar que los controles sean eficaces, que los procesos se ejecuten según fueron diseñados, y se aseguren que los niveles de riesgo se localizaran dentro del apetito de riesgo de la empresa.
http://www.isaca.org/chapters7/Madrid/members/Pages/Publicaciones.aspx

7. El Programa de Aseguramiento / Auditoría de Privacidad de Datos. Marzo 2018. ISACA.
Este libro ha sido traducido por un equipo de ISACA en el que he participado. El Programa de Aseguramiento / Auditoría de Privacidad de Datos comparte los objetivos de control y los controles en áreas de privacidad de datos que comienzan con la recopilación de datos a través de la gestión de incidentes. El objetivo principal es proporcionar a las organizaciones un medio para evaluar la efectividad de sus prácticas en torno al gobierno de los datos para la privacidad, confidencialidad y cumplimiento (DGPC).
http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/data-privacy-audit-program.aspx

8. La Nueva Economía de la Defensa en un Nuevo Orden Mundial. - Reflexiones desde el Ámbito Aeroespacial. Capítulo 10, Págs. 253-272. Editorial Ministerio de Defensa. Marzo 2018.
Esta obra refleja los contenidos de las Jornadas Aeroespaciales de Economía de la Defensa del Ejército del Aire. Un esfuerzo coordinado entre universidad, empresa y administración, en el que expertos de estos sectores revisan conceptos tradicionales y los actualizan, conscientes de que sólo desde una visión conjunta se encontrarán soluciones eficaces a desafíos tan complejos. Iniciativas como estas Jornadas acercan a la sociedad un campo del conocimiento tan importante como el de la Economía de la Defensa, constituyendo un ejemplo de otro de los pilares de la acción del Ministerio de Defensa, la Cultura de Defensa.
http://www.ejercitodelaire.mde.es/EA/ejercitodelaire/es/.galleries/anexos/La-Nueva-Economia-de-la-Defensa-en-un-Nuevo-Orden-Mundial.pdf

9. Los estudios militares y de seguridad en los albores del siglo XXI. Modelo de gestión del conocimiento económico basado en el marco input output. Un caso de estudio aplicado al sector de la defensa en España. ISBN 978-84-338-6085-9, págs. 473-491. Editorial Universidad de Granada. Junio 2017.
La obra reúne las aportaciones de numerosos expertos y grupos de investigación de diferentes universidades, centros de investigación españoles y extranjeros. Recoge el esfuerzo de investigadores civiles y militares, reunidos en torno a las mismas preocupaciones. Constituye un material relevante, de gran valor intelectual, de plena actualidad, minucioso, analítico y con aportaciones muy novedosas a los campos de la seguridad y de la defensa, desde diferentes disciplinas como la Economía, la Ciencia Política la Historia, la Ingeniería y la Sociología. En el capítulo de libro se expone el modelo MOCIE para el impacto económico de los programas públicos y su aplicación al sector de la defensa en España. https://dialnet.unirioja.es/servlet/libro?codigo=693346

10. Modelo de Gestión del Conocimiento para el Impacto Económico. Aplicación al sector Defensa. TESIS DOCTORAL. Departamento de Economía Aplicada VI. Universidad Complutense de Madrid. Abril 2016.
En el escenario actual macro económico la toma de decisiones en materia económica de cualquier entidad pública debe de estar sustentada por una adecuada inteligencia económica. Es prioritario disponer de modelos, técnicas y herramientas que permitan garantizar un control adecuado en todas sus inversiones. En la presente tesis se expone un modelo de gestión del conocimiento basado en el marco input output, que nos permite conocer el impacto económico de las inversiones realizadas. Este modelo está soportado por un sistema de información que coadyuvará a los analistas económicos para la toma de decisiones en el campo de las inversiones públicas. El modelo y el sistema se han aplicado en el área de la Defensa al objeto de conocer el impacto económico de una serie de programas de inversión en el sector aeronáutico. http://eprints.ucm.es/40568/

11. Transformando la Ciberseguridad. Noviembre 2015. ISACA. ISBN 978-1-60420-387-5.
Este libro ha sido traducido por un equipo de ISACA Madrid en el que he participado. Se trata de una publicación que está pensada para múltiples audiencias que están tratando con la ciberseguridad directa o indirectamente. Estas pueden incluir responsables de seguridad de la información, gerentes de seguridad corporativos, usuarios finales, proveedores de servicios, administradores de TI y auditores de TI. El propósito es permitir un marco uniforme de gobierno, gestión de riesgos y gestión de seguridad para las empresas y otras organizaciones.
http://www.isaca.org/COBIT/Pages/DownloadProduct.aspx?pc=WCB5TCS1

12. COBIT 5 for Information Security (Spanish). Enero 2014. ISACA. Código del Producto: CB5ISS.
Este libro ha sido traducido por un equipo de ISACA Madrid en el que he participado. Se trata de una Guía Profesional desde el punto de vista de la seguridad, mirando con un prisma de seguridad de la información a los conceptos, catalizadores y principios de COBIT 5. Este libro pretende ser un marco "paraguas" para enlazar con otros marcos de seguridad de la información, buenas prácticas y estándares. Describe la omnipresencia de la seguridad de la información en toda la empresa y ofrece un marco general. Los marcos, buenas prácticas y estándares relevantes de seguridad de la información tienen que ser ajustados para adaptarse a requerimientos específicos del entorno específico de la empresa. El lector puede entonces decidir, basándose en las necesidades específicas de la empresa, qué marco o combinación de marcos es mejor usar, también teniendo en cuenta la situación histórica de la empresa, la disponibilidad del marco y otros factores.
http://www.isaca.org/COBIT/Pages/COBIT-5-spanish.aspx

13. COBIT 5 Enabling Processes (Spanish). Enero 2013. ISACA. ISBN 978-1-60420-285-4.
Este libro ha sido traducido por un equipo de ISACA Madrid en el que he participado. El libro "COBIT 5: Procesos Catalizadores" complementa a COBIT 5. Esta publicación contiene una guía de referencia detallada de los procesos que están definidos en el modelo de procesos de referencia de COBIT. El marco COBIT 5 se construye sobre principios básicos, que quedan cubiertos en detalle e incluyen una guía exhaustiva sobre los catalizadores para el gobierno y la gestión de las TI.
http://www.isaca.org/COBIT/Pages/COBIT-5-spanish.aspx

---

14. La Ciberseguridad Nacional, un compromiso de todos. SCSI junio 2012.
Dentro del marco del Instituto Español de Ciberseguridad (SCSI, Spanish Cyber Security Institute) e ISMS Forum, se ha realizado un estudio en el cual se desarrolla una aproximación a los conceptos de ciberespacio y ciberseguridad, a los riesgos y amenazas conocidos, a la gestión existente en España y a la necesidad de desarrollar un sistema nacional de ciberseguridad que fomente la integración de todos los actores e instrumentos, públicos o privados, para aprovechar las oportunidades de las nuevas tecnologías y hacer frente a los retos que presentan. En el estudio se enumeran y definen las principales funciones que debe tener asignada la Ciberseguridad Nacional, se detallan los habilitadores de la ciberseguridad, se propone una estructura organizativa, se marcan los objetivos principales de la Ciberseguridad Nacional para el periodo 2012-2015 y se enumeran un conjunto de acciones que permitirán alcanzar dichos objetivos.
https://www.ismsforum.es/ficheros/descargas/informe-scsi1348666221.pdf

---

14. National Cyber Security, a commitment for everybody. SCSI. Junio 2012.
Information and Communications Technology (ICT) have contributed to the welfare and progress of societies, in such a way that a large part of public and private relations depends on these technologies. Over time and throughout evolution risks have emerged that have made it necessary to manage the ICT security. Initially cyber security was concerned with protecting information reactively, although subsequently it has evolved towards a proactive position, which identifies and manages risks that threaten cyber space. Within the framework of the SCSI (Spanish Cyber Security Institute) and ISMS Forum, a study was carried out which developed an approach to concepts of cyber space and cyber security. The main conclusions obtained from the study are summarized in this document.
http://www.ismsforum.es/ficheros/descargas/a-national-cyber-security-strategy-.pdf

---

15. Desarrollo de un servicio de notificación de cambios en una base de datos de gestión de la configuración mediante programación generativa. TESIS DOCTORAL. Universidad Nacional de Educación a Distancia. Escuela Técnica Superior de Ingeniería Informática. Departamento de Ingeniería de Software y Sistemas Informáticos. 02/2011. http://e-spacio.uned.es/fez/eserv.php?pid=tesisuned:IngInf-Jrcoz&dsID=Documento.pdf

---

16. Modelo de Madurez para la Privacidad de una Red Social Virtual. Febrero 2010. José Ramón Coz y Enrique Fojón Chamorro. ISBN: 978-1-4457-2017-3.
Este libro presenta los aspectos más relevantes relacionados con la privacidad de la información de las redes sociales virtuales. la obra presenta un modelo de madurez que permite valorar la red social virtual en esta materia. el libro está orientado, tanto a los profesionales de tecnologías de la información interesados en profundizar en esta materia, como a los propios usuarios de las redes sociales virtuales que estén preocupados por la privacidad de su información.
http://www.amazon.com/MODELO-MADUREZ-PRIVACIDAD-VIRTUAL-Spanish/dp/1445720175

---

17. Electronic Notes in Theoretical Computer Science (ENTCS), Vol. 238, N. 2, 06-2009. 25-34.
Capítulo de Libro sobre programación Generativa mediante el Lenguaje EFL (Exemplar Flexibilitation Language). http://portal.acm.org/citation.cfm?id=1555111

---

18. Marco para la Auditoria de los Sistemas de Información. Editado por ISACA MADRID. (2009).
ISBN: 978-84-613-4128-3.
Una de las labores que tradicionalmente ha realizado ISACA® ha sido la publicación de materiales que guiaran a los auditores de sistemas en la realización de sus trabajos de auditoría. Así, se ha desarrollado todo un cuerpo normativo que incluye Estándares, Guías y Herramientas y Técnicas. Estos más de cincuenta documentos, en su versión original proporcionan: a los auditores, los niveles mínimos de calidad que debe reunir su trabajo para cumplir con su responsabilidad profesional; a la Dirección y a terceros de cualquier tipo interesados en la función de auditoría, bases para la generación de expectativas adecuadas. En definitiva, un conjunto de materiales que merece la pena reunir en una obra de referencia que pueda ser utilizada como fuente de consulta para todos aquellos que tengan alguna relación con la auditoría de sistemas.
http://www.revistasic.com/revista87/otrostitulos_87.htm

---

19. Advanced Software and Control for Astronomy II. Edited by Bridger, Alan; Radziwill, Nicole M. Proceedings of the SPIE, Volume 7019, pp. 70191L-70191L-9. ISBN-10: 0819472298. (2008).
Capítulo de Libro sobre programación generativa utilizada en sistemas de adquisición de datos en astronomía.
http://adsabs.harvard.edu/abs/2008SPIE.7019E..52L

COLABORACIÓN CON GRUPOS, REVISTAS Y PUBLICACIONES

- **Miembro del Comité Editorial** de las siguientes revistas científicas y de investigación:
  - Mediterranean Journal of Basic and Applied Sciences. ISSN: 2581-5059. URL
  - Asian Journal of Basic Science & Research (AJBSR). ISSN: 2582-5267. URL
  - Open Access Journal of Applied Science and Technology (OAJAST). ISSN: 2993-5377 URL
  - Cyber Security: A Peer-Reviewed Journal. ISSN: 2398-5100 (print), 2398-5119 (web) URL
  - Journal of Marketing & Supply Chain Management. ISSN: 2754-6683. URL
  - International Journal of Applied Science and Research (IJASR). ISSN:2581-7876. URL
  - Transactions on Applied Science, Engineering and Technology (TASET). URL
  - Journal of Applied Surface Science (JASS). ISSN: 2993-5326. URL

- **Revisor de Revistas Científicas y de Investigación**, como Knowledge Management Research & Practice, British Journal of Economics, Management & Trade, Journal of Global Economics, Management and Business, International Scholars Journals, Journal of Basic and Applied Research international, British Journal of Mathematics & Computer Science, Advances in Research, British Journal of Applied Science & Technology, Asian Journal of Economics, Business and Accounting, Journal of Supercomputing, Asian Journal of Research in Computer Science, Asian Journal of Pure and Applied Mathematics, Asian Journal of Advances in Research o BP International or Journal of Advances in Mathematics and Computer Science.

- **Certificados de Excelencia como Revisor** otorgado por diversas revistas cientificas como la revista Asian Research Journal of Mathematics (URL), la revista Journal of Energy Research and Reviews (URL), la revista Asian Journal of Research in Computer Science (URL), la revista BP International (URL), la revista Journal of Economics, Management and Trade (URL), la revista Asian Journal of Pure and Applied Mathematics (URL), la revista Journal of Engineering Research and Reports (URL) o la revista Journal of Advances in Mathematics and Computer Science (URL).

- **Investigador desde 2016** en el Departamento de Economía Aplicada, Pública y Política **(**URL**)** de la **Universidad Complutense de Madrid.** Resumen con las principales colaboraciones realizadas hasta la actualidad: https://produccioncientifica.ucm.es/unidades/1263/colaboracion/investigador/4274749

PATENTES - REGISTRO DE LA PROPIEDAD INTELECTUAL

- Registro de la propiedad intelectual: **Modelo de Madurez de una Red Social Virtual en materia de Privacidad. Cuadro Integral de Mandos como soporte a la evaluación del modelo**. Número de expediente 12/RTPI-009226/2009. Referencia: 12/070438.8/09.

- **EFL. Exemplar Flexibilization Language**. Implementación en Ruby del lenguaje de flexibilización de ejemplares. Se trata de un lenguaje diseñado para la generación automática de código publicado bajo licencia GNU, General Public License (LGPL). Se han publicado tres versiones de esta implementación, disponibles como Gemas de Ruby:
  - https://rubygems.org/gems/EFL/versions/1.0 , del 15 de Noviembre de 2007
  - https://rubygems.org/gems/EFL/versions/1.0.1, del 18 de Febrero de 2008
  - https://rubygems.org/gems/EFL/versions/1.0.2, del 14 de Abril de 2009

ENLACES SOBRE ACTIVIDAD CIENTÍFICA E INVESTIGADORA

- Conferencia ENISE 18 organizada por INCIBE. León. Octubre 2024. URL
- Curso de Verano organizado por la Universidad Complutense de Madrid en El Escorial. Julio 2024. Resumen del curso: URL
- Conferencia sobre la experiencia de la Agencia Espacial Europea de las auditorias en el sector de la navegación. Noviembre 2023. Resumen de las jornadas, URL
- Seminario de la Cátedra del Almirante Don Juan de Borbón sobre el Arma Económica y el sector del espacio. Mayo 2023. URL
- Jornada sobre el empleo en el sector espacial organizada por la Universidad Europea del Atlántico. Mayo de 2023. URL
- Evento C-Meet sobre Innovación y Digitalización organizado por la CEOE de Cantabria en Septiembre de 2022. URL del evento. Presentación. Conferencia. Entrevista.
- Conferencia en la tercera edición del Webinar de Ciencias Aplicadas, Ingeniería y Tecnología (V-Applied2022) sobre la logística en ciber-auditorias complejas. Febrero 2022. URL
- Conferencia sobre la problemática de la logística en las ciber-auditorias del sector espacial en el Evento organizado por la ISACA Madrid en Junio de 2021. URL
- Artículo sobre la auditoria del Gobierno TI en el sector de la navegación en la ISACA Journal, news and trends. URL
- Conferencia en la tercera edición del Webinar de Ciencias Aplicadas, Ingeniería y Tecnología (V-Applied2021) sobre la planificación de ciber-auditorias complejas. Marzo 2021. URL
- Conferencias sobre las lecciones aprendidas sobre planificación de auditorías en entornos internacionales en el Congreso de ISACA Iberoamérica 2020. 26-30 de Octubre de 2020. URL
- Artículo sobre la ejecución de ciber-auditorias en la revista Cyber Security: A Peer-Reviewed Journal. Volume 4. Noviembre 2020. URL
- Conferencia sobre el sector de la navegación y la ciberseguridad en la Infosecurity ISACA North America Expo and Conference. New York, USA, 18-20 Noviembre 2019. URL
- Conferencia sobre las ciber-auditorias en el sector de la navegación en la *EuroCACS/CSX Conference. Geneva, Switzerland, 16-18 October 2019.* URL
- Revista de Economía Industrial Núm.412: Industria de Defensa. Páginas 57 – 65. Septiembre 2019. URL
- XXX Congreso Global de Ciberseguridad, Seguridad de la Información y Privacidad, SECURMATICA, Abril 2019. Conferencia sobre ciberseguridad en entornos críticos. URL
- El papel de la ciberseguridad en la gestión comunicativa en las organizaciones. INNOVATIA. Feb 28, 2018. URL
- Conferencia sobre la gestión del conocimiento económico en la nueva economía de la Defensa. Jornadas Aeroespaciales de Economía de la Defensa del Ejército del Aire. Marzo 2017. URL.
- Conferencia sobre el Modelo de gestión del conocimiento económico basado en el marco input output (MOCIE). Congreso Internacional de Estudios Militares. CIdEM 2016. Octubre 2016. URL.
- La incubadora de proyectos de ciberseguridad de la OTAN y otras iniciativas internacionales. Septiembre 2016. URL.
- Ciberseguridad nacional, una necesidad. El español. Noviembre 2015. URL.
- No sé lo que pasa en mi red. ¿Puedo protegerla adecuadamente? CIBER – Real Instituto Elcano. Octubre 2015. URL.
- Herramienta de Autoevaluación de la Madurez en Gobierno TI basada en COBIT-PAM. Comisiones ISACA. Septiembre 2015. URL.
- La Ciberdefensa militar ante el reto de Internet de las Cosas. Revista SIC. Sept.2015. URL.
- Los Ciber-comandos y la Segregación de Funciones. Real Instituto Elcano. Junio 2015. URL.
- ISAC como punto de unión de las arquitecturas en Ciberdefensa. Revista SIC. Abril 2015. URL.
- Sin coordinación efectiva no hay Ciberdefensa. Real Instituto Elcano. Abril 2015. URL.
- Las diferentes velocidades de la ciberdefensa en el ámbito de la OTAN. THIBER - El Mundo. Marzo 2015. URL.
- Los perfiles de Ciberseguridad, bajo demanda. Revista INNOVATIA. Febrero 2015. URL.
- STIX: ¿el estándar para la compartición de la información de la ciberdefensa? Revista SIC. Febrero 2015. URL.
- ¡El Ciber Reino unido, una gran apuesta por la Ciberseguridad y la Ciberdefensa! ISMS Forum. Enero 2015. URL.

- II Edición del Estudio del Estado del Arte de la Seguridad en la Nube. ISMS Forum. Cloud Security Alliance España. Noviembre 2014. URL. PDF.
- ¡Arabia Saudí, el país del petróleo, y la Ciberseguridad! ISMS Forum. Noviembre 2014. URL.
- El reto de la compartición de información en Ciberdefensa. Revista SIC. Nov.2014. URL. PDF.
- Francia, un Liderazgo en Ciberdefensa. ISMS Forum. Octubre 2014. URL.
- Entornos de Sistemas Multiagente y Ciber-Físicos en la Ciberdefensa. Revista SIC. Septiembre 2014. URL. PDF.
- Las embajadas de datos: la protección de la información estatal. THIBER. ARI 36/2014. 16/7/2014. URL. PDF.
- El capítulo español del Cloud Security Alliance traduce al español la versión 3d del Cloud Controls Matrix y la adapta a la LOPD y al Esquema Nacional de Seguridad (ENS). Madrid, June 2014. URL
- Presentación sobre las cibercélulas: una capacidad para la ciberseguridad y la ciberdefensa nacionales'. Presentación en formato Prezi exportable (auto ejecutable). Madrid, 2013. URL
- Expertos reunidos por ISMS Fórum debaten el estado actual de nuestra ciberseguridad nacional. Madrid, octubre 2013. URL
- Retraso de la Estrategia Nacional de Ciberseguridad en España. Madrid, octubre 2013. URL
- Ideas clave sobre la Estrategia Nacional de Ciberseguridad en España. Madrid, 10-2013. URL
- Breve análisis sobre la Nueva Estrategia de Ciberseguridad Nacional. Diciembre 2013. URL
- Modelos y enfoques de ciberseguridad en las redes sociales virtuales. RED SEGURIDAD. Madrid septiembre 2013. URL
- Cyber cells: a tool for national cyber security and cyber defense. Real Instituto Elcano. Septiembre 2013. URL. PDF.
- Las cibercélulas: una capacidad para la ciberseguridad y la ciberdefensa nacionales. Real Instituto Elcano. Julio 2013. URL. PDF
- Cost Models and Productivity Building Applications Based on the Notification of Changes in Databases. SUMMARY. PAPER.
- A Domain Engineering Approach to Increase Productivity in the Development of a Service for Changes Notification of the Configuration Management Database. Journal of Software Engineering and Applications. April 2013. SUMMARY. PAPER
- Retos de la "conciencia situacional" en la Ciberdefensa. Revista SIC. Abril 2013. URL. PDF
- La conciencia situacional en la Ciberdefensa. Revista SIC. Febrero 2013. URL. PDF
- Expertos en delincuencia informática piden que se adapte la normativa en el I Foro de la Ciberseguridad. URL
- Evaluación de la privacidad de una red social virtual". Revista RISTI nº 9, 6-2012. ISSN 1646-9895. ARTICULO.
- La Ciberseguridad Nacional, un compromiso de todos. SCSI Junio 2012. URL
- La Geoestrategia del Conocimiento en Ciberseguridad". Revista RED SEGURIDAD. URL
- Panorama Internacional en el establecimiento de Estrategias Nacionales de Ciberseguridad. Revista SIC. Junio 2011. URL
- Artículo Publicado en el V Congreso de itSMF 2010 sobre Privacidad en las Redes Sociales y ponencia en dicho Congreso. URL. Congreso. Ponencia.
- Electronic Notes in Theoretical Computer Science, Volume 238, Number 2, June 2009. URL
- Seminario en la Universidad de Oxford sobre la Generación de Código con EFL. URL
- A first-generation software product line for data acquisition systems in astronomy. URL

ACTIVIDAD DOCENTE

Más de quince (15) años de experiencia docente en diversas entidades, escuelas de negocio y universidades (a tiempo parcial), que incluyen la Universidad Internacional de la Rioja (UNIR), la Universidad Complutense de Madrid (UCM), el Centro Universitario ISEN de la Universidad de Murcia, el Centro Superior de Estudios de Defensa Nacional (CESEDEN), la Asociación de Auditores de Sistemas o la Escuela de Negocios Internacional (IIBS), entre otros. Durante este periodo se ha impartido docencia sobre **Auditoria de Sistemas, Control de Tecnologías de la Información, Continuidad de Negocio y Recuperación de Desastres, Seguridad de la Información, Gestión de Servicios TI, Criptología, Metodologías de desarrollo software, Impacto Económico, Gestión de Programas y Proyectos o preparación para diversas certificaciones internacionales** como COBIT, CISA, CISM, CISSP, CGEIT, ITIL, MSP, PRINCE2 o ISO20000.
\\

ASIGNATURAS Y CURSOS IMPARTIDOS

- **Profesor de varias asignaturas de ciencia y tecnología. Preparación para el título oficial de Formación Profesional**. Regimiento de Caballería del Ejército de Tierra. Valladolid. Ministerio de Defensa. Agosto 1996 – Diciembre 1996. 100 Horas acreditadas por el Ministerio de Educación.

- **Impartición de varios cursos sobre Bases de Datos y Programación orientadas a objetos:** CORBA, C++, C, Object Store, Oracle. Empresa Ideal Objects S.A. Octubre 1997 - Febrero 1998. Madrid. 120 Horas en total.

- **Impartición de varios cursos sobre Análisis y Programación orientadas a objetos:** UML, C++, Java, .NET, . Grupo FCC. División ESPELSA. Junio 1998 – Diciembre 2002. Madrid. 120 Horas en total.

- **Impartición de varios cursos en el Ministerio de Defensa a responsables de contractos técnicos y responsables de sistemas**. Inspección General CIS y Centro Superior de Estudios de Defensa Nacional (CESEDEN). Madrid. Septiembre 2003 – Septiembre 2005.
  - Cursos sobre la Calidad del Software: CMMI, PECAL, SPICE, ISO 12207. 120 Horas total.
  - Cursos sobre Gestión de Datos en Defensa: bases de datos, data mining, data warehouse, NATO Data Management Policy. 120 Horas en total.
  - Curso sobre Gestión de Servicios TI en Defensa: ITIL, ITSM, ISO20000, TCO, eTOM. 120 Horas total.
  - Curso sobre Arquitectura SOA y Servicios Web: XML, UDDI, SOAP, WSDL. 40 horas en total.

- **Profesor en la Information Systems Audit and Control Association (ISACA) para la preparación de certificaciones oficiales**, durante el periodo Septiembre 2005 - Junio 2016. Cursos organizados por el capítulo de ISACA Madrid. Los cursos se dieron en multitud de centros y empresas, en diversas localizaciones de la Comunidad de Madrid.
  - Preparación para la Certificación **CISA** (Certified Information Systems Auditor) de la ISACA: auditoria, COBIT, metodologías de desarrollo SW, gestión de proyectos TIC y gestión de servicios TIC. Total, unas 240 horas.
  - Preparación para la Certificación **CISM** (Certified Information Security Manager) de la ISACA: continuidad de negocio y recuperación de desastres, seguridad de la información y criptología. Total, unas 60 horas.

- **Profesor en la Escuela de Negocios Internacional (IBBS) y el Instituto Innove**, en los centros de León y Madrid, durante el periodo de Septiembre de 2007 a Septiembre de 2017. Seminarios y asignaturas impartidas durante este periodo: Auditoria de Sistemas, Gobierno y Control TIC, Continuidad de Negocio y Recuperación de Desastres, Seguridad de la Información, Gestión de Servicios TI y Metodologías Software. Total, unas 300 horas.

- **Profesor en NEMIND, actualmente parte del grupo BTS, para la preparación de las certificaciones oficiales CISSO y CISSP.** Madrid. Septiembre 2003 – Septiembre 2005.
  - Preparación para la Certificación: Certified Information Systems Security Officer (**CISSO**). Certification granted by the NICCS (National Initiative for Cybersecurity Careers and Studies). Total, unas 40 horas.
  - Preparación para la Certificación: Certified Information Systems Security Professional (**CISSP**), certification granted by the International Information System Security Certification Consortium, also known as (ISC)². Total, unas 80 horas.

- **Impartición de una serie de Seminarios sobre el impacto económico del sector espacial** para el Máster en Logística y Gestión Económica de la Defensa de la Universidad Complutense de Madrid (URL), para la Cátedra Almirante Juan de Borbón (URL) y para el Centro Universitario ISEN de Cartagena (URL)**.** Desde junio de 2021 hasta la actualidad.

- Impartición de dos conferencias sobre ciberseguridad, auditorias y empleo en el sector especial durante **el curso de verano "El universo a nuestro alcance: el auge de las ciencias del espacio en España",** organizado por la Universidad Complutense de Madrid, en El Escorial, Madrid, en Julio de 2024 (URL).

- **Profesor en la Universidad Internacional de la Rioja (UNIR).** Desde el curso académico 2020-2021 hasta la actualidad, **responsable de la asignatura de Gestión Tecnológica** en la Facultad Superior de Ingeniería y Tecnología (ESIT). La asignatura cubre la auditoria de sistemas, la gestión de riesgos y sus herramientas asociadas, la continuidad de negocio conforme a la norma ISO22K, la gestión de seguridad de la información conforme a la serie ISO27K, los modelos de madurez CMMI, el Gobierno TI según COBIT y la gestión de la calidad TIC (URL).

- Miembro del Claustro de la Facultad Superior de Ingeniería y Tecnología en la Universidad Internacional de la Rioja para el Máster en Dirección de TI desde el curso académico 2020-2021 (URL)

ESTANCIAS COMO PROFESOR VISITANTE

El Programa de Profesores Visitantes tiene como objetivo facilitar que los distintos centros de las Universidades puedan invitar a investigadores/as residentes en el extranjero con relevancia en sus respectivos ámbitos del conocimiento. Se han realizado dos estancias como profesor visitante en las siguientes universidades:

- **Profesor visitante en la Universidad Europea del Atlántico** (URL). Santander, en Mayo de 2023. Como parte de la estancia, se participó en la cuarta sesión de las jornadas de empleo que organiza la universidad y se impartió una conferencia donde los estudiantes tuvieron la oportunidad de aprender un poco más sobre la industria espacial europea, la ciberseguridad y las auditorías, así como de las oportunidades de trabajo que se encuentran disponibles. Noticia sobre el evento: URL

- **Profesor visitante en la Escuela Técnica Superior de Náutica de la Universidad de Cantabria** (URL)**.** Santander, en Septiembre de 2024. Como parte de la estancia, se realizaron diversos seminarios científicos sobre los programas de la Agencia Espacial Europea, el sector de la Navegación y la Ciberseguridad. Además, se realizó una conferencia a los alumnos sobre el empleo en el sector espacial y de la ciberseguridad. Comunicación sobre la visita: URL. Noticias sobre la visita: URL

PROGRAMAS UNIVERSITARIOS DE RADIO

1. Seguridad y control de acceso basado en sistemas biométricos.
Coz, J.R.; Heradio, R.; Estívariz, J. F. Emitido por RADIO 3 (RNE) el 26/03/2008.
Canal UNED: http://unedradio.blogspot.com/2008/03/la-ingenieria-de-software-y-sistemas.html
Audio: http://teleuned.uned.es/realaudiocemav/2007_2008/2008_03/20080326_02.wma
En este programa se debaten cuestiones sobre la seguridad de la información, la privacidad y el Control de accesos basados en sistemas de tipo biométrico. Se exponen algunos ejemplos de uso como el DNI o los pasaportes electrónicos.

---

2. Historia de la Criptología y su Evolución.
Coz, J.R.; Heradio, R.; Fdez. Amorós, David. Emitido por RADIO 3 (RNE) el 23/11/2011.
Audio: http://cozweb.es/radio/cripto1.mp3
Ficha Técnica: http://cozweb.es/radio/cripto1.pdf
En este programa se introducen los conceptos básicos sobre la Criptología y sus disciplinas asociadas, el Criptoanálisis, la Esteganografía y la Criptografía. Además, se hace un breve resumen histórico de su evolución.

---

3. Criptología actual y Ciberseguridad.
Emitido por RADIO 3 (RNE) el 30/11/2011.
Audio: http://cozweb.es/radio/cripto2.mp3
Ficha Técnica: http://cozweb.es/radio/cripto2.pdf
En este programa se introducen algunos avances sobre la Criptología y se repasan las cuestiones más relevantes sobre la seguridad nacional en el ciberespacio (la Ciberseguridad).

DIRECCIÓN DE TRABAJOS FIN DE MASTER

Desde el curso académico 2020-2021 hasta la actualidad, **Director de Trabajos Fin de Master (TFM) en la Facultad Superior de Ingeniería y Tecnología** (ESIT) de la Universidad Internacional de la Rioja (UNIR). Se ha llevado a cabo la dirección de trabajos en los siguientes Máster:

- **Máster Universitario en Ciberseguridad**. URL. Se han tutorizado, hasta la fecha, **un total de 36 Trabajos Fin de Máster**. Títulos de los TFM tutorizados:
  - *Nueva metodología para la protección de la información aplicada a dispositivos móviles Android.* R.H. Cuvi Vargas.
  - *Ataques al protocolo de autenticación OPENID CONNECT + OAUTH2.* C.A. Quiñonez Murillo
  - *Metodología para la implementación de software Seguro ERP E-CABILDO para Gobiernos Municipales.* J.W. Sandoval Paspuel
  - *El nivel de alineamiento de la regulación financiera en el Perú conforme al marco de trabajo de Ciberseguridad de NIST.* E.A. Rojas Gonzales.
  - *Desarrollo de una guía para la gestión del Malware en las empresas.* F. Campà Aubets
  - *Diseño de una Metodología para el análisis de Riesgos Inherentes y Residuales a partir del mapeo del marco CSF NIST y la Matriz MITRE ATT&CK.* H.Y. Ortiz Pérez.
  - *Metodología de Red Team con base a ataques informáticos en empresas.* V.M. Ramírez Medina.
  - *Propuesta de nuevo protocolo para la implantación y uso de TLS 1.3.* H.E. Quiroga González.
  - *Construcción de un protocolo de apoyo a la concesión de créditos soportado por herramientas OSINT y aplicación a un caso de uso.* L.D. Jiménez Terrazas
  - *Propuesta de metodología de Auditoria Técnica de Seguridad aplicable a entidades del sector Financiero en Colombia.* J.D. Caro Quiroga.
  - *Creación de un Proceso de Auditoría de Seguridad Técnica basada en la matriz MITRE ATTACK y NIST CSF.* K.S. Salazar Espinosa.

- *Propuesta de metodología para el cumplimiento de las guías del MSPI en el Sector financiero.* A.M. Guevara Mera.
- *Blockchain en gestión de riesgos, detección del fraude e implantación de requisitos (KYC) y Framework*. C.J. Sánchez Gómez.
- *Desarrollo de un método ágil para la implantación un sistema de gestión de seguridad de la información en el sector de empresas privadas pequeñas y medianas TICS.* L. Chávez Pérez.
- *Metodología integral para la seguridad de la información basados en los estándares ISO 27001, ISO 22301 e ISO 31000 para la EFR.* R.G. Quecan Fetecua
- *Piloto experimental sobre el Análisis de Riesgos Informáticos aplicando Reglas de Asociación y Desarrollo de Plan de Seguridad en empresas de consumo masivo.* V. Vélez Sarmiento
- *Formulación de una metodología para el fortalecimiento las redes de datos de la entidad DIAN.* A.C. Rodríguez Moyano
- *Portal informativo de ciberataques y relación de posibles soluciones.* J.L. Guaca Torres
- *Análisis de vulnerabilidades en Pymes mediante la exposición a la ingeniería social y propuesta de medidas de mitigación.* M. Saavedra Ortiz
- *Metodología para el desarrollo de políticas de seguridad conforme a normativa ISO 27001 para clientes de entornos cloud.* V.K. Rodríguez López
- *Metodología de Auditoría Continua para una Compañía de Seguros en Perú.* K.V. Salinas Ticona
- *Desarrollo de aplicación didáctica de métodos de cifrado.* O. Santos Bernabé
- *Desarrollo de un piloto experimental sobre un Lector Near Field Communication de tarjetas ENV.* J.M. Sierra Ramos
- *Piloto experimental sobre capacidad de exfiltración de datos del malware.* W.E. Silva Salas.
- *Crawler Web como Herramienta de Apoyo para el Proceso de Pentest web.* Y. Saavedra Guerrero
- *Evaluar el cumplimiento de la Ley Orgánica de Protección de Datos Personales (LOPDP) aplicando una red blockchain en el Hospital San Juan de la ciudad de Riobamba.* B.A. Giraldo Baquerizo, M.B. Villacis Rivera y J.J. Delgado Anchundia
- *Desarrollo de una herramienta de cifrado de archivos en la nube.* T. Kamisato Orellana
- *Desarrollo de Servicios Web REST "Inseguros" con Express.js: Explorando Vulnerabilidades y Soluciones.* D.A. Usca Farinango
- *Implementación de una plataforma ante incidentes informáticos y procedimientos de defensa.* D.M, Silva Gurrionero, S.A. Sánchez Gutiérrez y M.A. Carreño Vargas
- *Metodología de una gestión básica de seguridad para pequeñas empresas en Colombia.* J.D. Rúa Henao, A.F. Gonzalez Torres y D.F. Salazar Valdion
- *Prototipo para la Mitigación de ataques DDoS en el Programa Nacional AURORA.* G.E. Herrera Quispe
- *Metodología de implementación del SGSI basada en la ISO27001 en proveedores de TI.* L.A. Mendaño y C.A Damaceña Toaza.
- *Investigación sobre las metodologías y patrones de los ataques mediante botnet.* A. Díaz Artola
- *Análisis de Redes Sociales para detectar ciberdelitos usando técnicas de NLP y SNA.* E. Gutiérrez Pérez.
- *Propuesta de Implementación de la Arquitectura en la Nube para una Administración de Justicia Eficiente en el Poder Judicial.* M. J. Quispe Sandoval
- *Auditoría de seguridad a Smarts d.o.o.* F. Ortega Guardia.

- **Máster Universitario en Dirección y Gestión de Tecnologías de la Información (TI).** URL. Se han tutorizado, hasta la fecha, **un total de 20 Trabajos Fin de Máster**. Títulos de los TFM tutorizados:
  - *Transformación Digital de los Procesos Principales del "Hotel Quindeloma and Art Galery" de la Gestión TI Tradicional.* G. Tasiguano Simbaña, T. Landívar Moreno, R. Rivera Toala.
  - *Mejora de los Procesos de Gobierno de TI en una Empresa de Productos Alimenticios.* A.M. Espinosa Guaita.
  - *Construir una arquitectura TOGAF en base a un sistema SGSI.* R.A. Arguello Ruiz.
  - *Plan estratégico de TI para la empresa TRUSTHAB basado en la metodología PETI.* J.J. Peñaherrera Romero
  - *Sistema de Gestión de Continuidad de Negocio para la industria farmacéutica.* C.V. Pauta Cuji

- *Guía de Migración de Servidores de la empresa Farmaenlace de acuerdo con el tipo de Nube a una infraestructura VDC.* M.G. Inuca Morales
- *Mejora tecnológica de la atención al cliente en la Corporación Nacional de Electricidad Ecuador (CNEL-EP) en el sector de comercialización.* L.A. Guzmán Peña y E.L. Quichimbo Bermeo.
- *Implementación de un SGSI bajo la norma ISO 27001 en una fundación privada sin ánimo de lucro.* P.I. Bueno Martín
- *Implementación de un plan estratégico de TI para transformar digitalmente una Legal Tech.* O.G. Matos Godoy
- *Elaboración de un modelo para implantar una metodología ágil en la Dirección de Gestión Tecnológica de la Información de la Universidad de Guayaquil.* I. R. Pacheco Guerrero y J.X. Torres Reyes
- *Diseño de un plan estratégico de TI (PETI) en una empresa mediana de Hidrocarburos.* A.C. Claro Osorio
- *Implementación de una infraestructura de transmisión de datos e Internet para las Oficinas de Migraciones.* D. Dávila Villacorta y K.A. Morales Guerrero
- *Diseño de un gobierno de seguridad de TI basado en la norma ISO 27000.* R.D. Ullrich Estrella
- *Marco de trabajo en la implantación de las TIC en las empresas del sector público.* R. Caballero Tomás
- *Implementación de un Agregador para la venta online en Marketplace.* A. Lopez de Bikuña Alzola
- *Implantación de un área de gestión de servicios TI en una entidad pública.* F.J. Calatayud Cristóbal
- *Transformación digital en entidades deportivas.* C. E. Baz Hormigos
- *Revisión y adaptación de la nueva NIS2 al marco de control de auditoría de soporte al sector de la navegación.* L. H. Rodriguez Pineda.
- *Plan de Gobernanza de Tecnología enfocado en transformación digital para la Organización Internacional para las Migraciones en Ecuador*. J. F. López Dávila, D. A. Cifuentes Arias
- *Plan para la Creación de un SOC (Centro de Operaciones de Seguridad), para la Corporación de Promoción Económica CONQUITO, usando Metodologías Ágiles y Enfoque PMP.* A. A. Barzallo Bravo, E. A. Granja Herrera

- **Máster Universitario en Ingeniería del Software y Sistemas Informáticos.** URL. Se ha tutorizado, hasta la fecha, **un total de 5 Trabajos Fin de Máster**. Título del TFM tutorizado:
  - *Desarrollo de un aplicativo de soporte a un marco de control de auditoría de soporte al segmento terreno del sector de la navegación.* J. M. Frías Salvachua.
  - *Desarrollo de una Plataforma Basada en Microservicios para la Gestión y Análisis de la Calidad del Agua.* Frank Montalvo Ochoa
  - *Desarrollo e Implementación de un chat legal basado en inteligencia artificial y optimización de la interfaz de usuario en la empresa Legalti – Ecuador*. R. S. Noroña Echeverria, S. Morales Reinoso.
  - *LinkuyConnect: Aplicación Móvil de Código Abierto para el Monitoreo del Bienestar en Adultos Mayores.* N. D. Moreira Ledesma.
  - *Diseño y desarrollo de una aplicación Web para el manejo del área académica de la Corporación Educativa Emmanuell.* I. J. Gomez Leguizamón

---

ASISTENCIA A TRIBUNALES UNIVERSITARIOS

Desde enero de 2021 hasta la actualidad, **miembro de tribunales, como Presidente y Secretario, para la evaluación de Trabajos Fin de Máster en la Facultad Superior de Ingeniería y Tecnología** (ESIT) de la Universidad Internacional de la Rioja (UNIR), en el **Máster Universitario en Seguridad Informática**.

Proyectos de Innovación Docente

- Artículo sobre el nuevo espacio de educación superior en ciberdefensa en el ámbito internacional. Revista SIC. Junio 2016. URL.
- Mesa Redonda del Congreso ENISE sobre el Marco Legal de las Infraestructuras Críticas. Conferencia sobre un modelo educativo para una Estrategia Nacional de Ciberseguridad. URL
- Impacto de las certificaciones TIC en el empleo en época de crisis. León, abril 2011. URL
- Desarrollo de familias de productos de software desde un enfoque generativo. URL
- Proyecto de innovación docente consistente en la elaboración de los contenidos y materiales didácticos o docentes de la asignatura titulada Gestión Tecnológica en la Facultad Superior de Ingeniería y Tecnología (ESIT) de la Universidad Internacional de la Rioja (UNIR) y adaptación al Modelo de 4Ps. Realizado en el periodo Septiembre de 2022 - Junio de 2023.

OTROS DATOS DE INTERES

Membresías

- Miembro del ISMS Forum. URL
- Socio Senior Numerario de ATI (Asociación de Técnicos de Informática). URL
- Asociado a la Sociedad de Antiguos Alumnos del IDE – CESEM.
- Miembro de ISACA. URL
- Miembro Fundador de THIBER, Think Tank sobre Ciberseguridad. URL
- Miembro del Club Internacional BPM. URL

Perfiles en Redes Sociales

- ● Research-Gate, ● Google Academico, ● LinkedIn, ● ORCID, ● Publons, ● Academia
- ● Summary of CV INGLES ● CV en INGLES ● CV Reducido
- Enlace con algunas Conferencias en YOUTUBE