# Curriculum Vitae

# Dr. José Ramón Coz Fernández

Noviembre 2018

# Tabla de contenido


***INFORMACIÓN PERSONAL*** _____ 3

***BREVE RESUMEN CURRICULAR*** _____ 3

***EXPERIENCIA PROFESIONAL*** _____ 4

***ESTUDIOS Y FORMACIÓN*** _____ 7

***DOCTORADO*** _____ 7

***LICENCIATURAS Y MÁSTER*** _____ 7

***ESTUDIOS DE POST-GRADO*** _____ 8

***CERTIFICACIONES PROFESIONALES*** _____ 8

***CURSOS SOBRE SEGURIDAD Y ENTORNO OTAN*** _____ 11

***OTROS CURSOS*** _____ 13

***IDIOMAS*** _____ 14

***ACTIVIDAD INVESTIGADORA*** _____ 14

***ARTÍCULOS Y PUBLICACIONES*** _____ 14

***PONENCIAS EN CONFERENCIAS Y CONGRESOS*** _____ 20

***LIBROS Y CAPÍTULOS DE LIBROS*** _____ 21

***ENLACES SOBRE ACTIVIDAD CIENTÍFICA E INVESTIGADORA*** _____ 24

***OTROS DATOS DE INTERES*** _____ 26

# INFORMACIÓN PERSONAL


| | |
|---|---|
| **Nombre** | **Dr. D. JOSE RAMON COZ FERNANDEZ** |
| **Teléfono** | **+31 71 565 57 57** |
| **E-mail** | **jose.ramon.coz@esa.int** |
| **Nacionalidad** | ESPAÑOLA |
| **Fecha de nacimiento** | 16 – 06 – 1972 |
| **Web** | **http://www.cozweb.es/** |


# 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 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 una docena de certificaciones internacionales en Tecnologías de la Información y varios postgrados en Telecomunicaciones.
Tiene más de veinte años de experiencia en Tecnologías de la Información y las Comunicaciones, y más de quince años de experiencia en el campo de la Ciberseguridad.
En la actualidad, trabaja como Cyber Internal Auditor en la Agencia Espacial Europea, y es investigador en el Departamento de Economía Aplicada de la Universidad Complutense de Madrid. Es, además, profesor en varias instituciones, universidades y escuelas de negocio.
Ha realizado varias publicaciones científicas y de tecnología, es revisor de revistas internacionales de ciencia, economía y tecnología, y es miembro de varias comisiones y asociaciones de auditoria y tecnologías de la información.

# EXPERIENCIA PROFESIONAL

| | |
|---|---|
| Fecha (desde – a) | **Octubre de 2018 hasta la actualidad** |
| Nombre del contratista | **EUROPEAN SPACE AGENCY.** ESTEC. NOORDWIJK, PAISES BAJOS. |
| Cargo y nombre del puesto | **GNNS CYBER INTERNAL AUDITOR** |
| Principal actividad y responsabilidades | • Funcionario de la Agencia Espacial Europea.<br>• *Cyber Internal Auditor* del Directorado de Navegación.<br>• Mi papel principal lo establece la Política Cibernética de la Comisión Europea dentro del Programa Galileo.<br>• 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.<br>• Esta función tiene una línea de reporte directa al Director de Navegación. |

---

| | |
|---|---|
| Fecha (desde – a) | **Marzo de 2012 hasta la octubre 2018** |
| Nombre del contratista | **NATO COMMUNICATIONS AND INFORMATION AGENCY (NCIA).** BRUSELAS, LA HAYA.<br>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 100 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 conlleva la monitorización de la implementación de todos los proyectos en sus ámbitos técnicos, de aseguramiento de la calidad, financieros y de contratación.<br>• 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 da 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.<br>• **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**.<br>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.<br>• Participación en grupos de trabajo de apoyo a la Secretaría De Estado de Defensa.<br>• Estudios y proyectos de investigación económicos, Industriales y Estratégicos sobre el Sector Industrial de la Defensa.<br>• Colaboración con la Cátedra de Mercados y Política Industrial de Isdefe con el Instituto de Economía de Barcelona.<br>• Participación en la elaboración de Ofertas Internacionales para Naciones Unidas, la Unión Europea y la OTAN. |

---

| | |
|---|---|
| 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.**<br>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.<br>• Apoyo a la subdirección General de Registros de Apoyo a la Actividad Judicial en materia de Tecnologías de la Información. Metodologías y Buenas Prácticas. |

Gestión de Proyectos. PRINCE2, COBIT, 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.**<br>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:<br>  ○ Infraestructuras Críticas de Seguridad en España. Proyecto para la Comisión Europea.<br>  ○ Gestión de la Identidad digital (Seguridad 2020). Proyecto de I+D del Ministerio de Industria.<br>  ○ Proyectos Internacionales Clasificados de Seguridad en Inmigración, Gestión de Fronteras y gestión de Identidades.<br>• Miembro de la Oficina de Dirección del DNI Electrónico (proyecto de más de 120 M€):<br>  ○ Asesoramiento en la gestión del proyecto y control de la calidad.<br>  ○ Convenios Marco con otras instituciones como el MAP, Ministerio de Industria, Agencia Tributaria o la Fábrica de Moneda y Timbre.<br>  ○ Colaboración en las Auditorías de Seguridad y LOPD y acreditaciones (CNI / CNN / ITSEC).<br>• Apoyo al Servicio de Gestión de Proyectos del área de Informática del Cuerpo Nacional de Policía. Gestión Técnica de Proyectos.<br>• Estudio de Funciones TI en la Policía y asesoramiento en la implantación de las mejores prácticas (ITIL, COBIT, PRINCE2). |

---

| | |
|---|---|
| Fecha (desde – a) | **Enero de 2005 a noviembre 2005** |
| Nombre del contratista | **INSPECCIÓN GENERAL CIS DEL MINISTERIO DE DEFENSA**<br>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.<br>• Análisis de Impacto.<br>• Elaboración de Procedimientos y Planes de Emergencia.<br>• Diseño de Centros de Respaldo.<br>• Implementación de nuevas prácticas COBIT, ITIL y Normativas OTAN |

---

| | |
|---|---|
| Fecha (desde – a) | **Enero 2003 a enero 2005** |
| Nombre del contratista | **INSPECCIÓN GENERAL CIS DEL MINISTERIO DE DEFENSA**<br>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.<br>• Gestión y supervisión de los estudios de Mercado de Productos.<br>• Gestión y supervisión de la entrada en explotación de diversos sistemas de Información del Ministerio.<br>• Responsable de la Elaboración y Difusión de la Arquitectura Técnica.<br>• Colaboración con grupos OTAN de Arquitecturas Software.<br>• Colaboración con la Oficina de Datos del Ministerio de Defensa:<br>• Política de Datos del Ministerio.<br>• Guías de Uso y Normativas de Datos.<br>• Comité de Seguimiento del Centro Internacional de Desminado. |

---

| | |
|---|---|
| Fecha (desde – a) | **Mayo 2000 a marzo 2003** |
| Nombre del contratista | **CONSORCIO EUROFIGHTER**,<br>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 OTAN.<br>• 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.<br>• 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.<br>• Participación como analista en los Proyectos:<br>  o INTRANET de Argentaria.<br>  o Optimización de Bases de Datos.<br>  o Proyecto Gestión de Tarjetas Bancarias y Proyecto SIPYC.<br>• 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:<br>  o Cuentas de Crédito a Promotores.<br>  o Intranet bajo tecnología Lotus Notes.<br>• Migración a Java de las Aplicaciones Corporativas.<br>• 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++.<br>• Soporte de Entornos CORBA.<br>• Soporte de Bases de Datos Orientadas a Objetos (Object Store).<br>• 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.<br>• Apoyo técnico a la actividad comercial del Instituto.<br>• Diseño y formación sobre Productos de Bases de Datos a través de Internet.<br>• Consultoría sobre Sistemas Operativos, Navegadores y Mensajería electrónica. |

---

# ESTUDIOS Y FORMACIÓN

## DOCTORADO

| | |
|---|---|
| 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. En la actualidad 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.<br>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 2004 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. Campos de la investigación: seguridad de la información, bases de datos, programación generativa, modelos económicos y líneas de productos software.<br>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.<br>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.<br><br>NOTA: Seleccionado en el Top 20 del Ranking Mundial de Masters en Logística y Gestión Económica. ENLACE |

| | |
|---|---|
| Fecha (desde – a) | SEPTIEMBRE 1990 A SEPTIEMBRE 1995 |
| Nombre de la Universidad | **UNIVERSIDAD DE CANTABRIA. Facultad de Ciencias.** |
| Estudios principales | Licenciatura en Ciencias Físicas.<br>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.<br>• Métodos de Planificación y Control en la Administración Pública.<br>• Diseño e Implantación de Proyectos de e-administración.<br>• Gestión de los Recursos Humanos en las Administraciones Públicas.<br>• Gestión de Proyectos Tecnológicos. Gestión de Sistemas de Información.<br>• Fundamentos de Métodos Cuantitativos para la Economía y la Empresa. |
| Título o Certificado | **GRADUADO ESPECIALISTA EN GESTION DE LA ADMINISTRACION PÚBLICA**<br>**http://www.cepade.es/formacion/Graduaciones1e.asp?anno=2005** |

| | |
|---|---|
| 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.<br>• Seguridad Informática. Los Sistemas de la Información.<br>• Habilidades Directivas. Gestión Financiera y Económica.<br>• Gestión de Recursos Humanos del Departamento de Informática.<br>• Explotación y Control. E – Business.<br>• Dirección y Gestión de Proyectos. Auditoria.<br>• Dirección de Equipos. Desarrollo de Sistemas.<br>• Comunicaciones y Comunicaciones Avanzadas.<br>• Proyecto Fin de Máster: *"Modelo Tecnológico y Normativo para una gran Corporación".* |
| Título o Certificado | **MÁSTER DE DIRECCION DE TECNOLOGIAS DE LA INFORMACION**<br>(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.<br>• Sistemas y Redes de Comunicaciones TCP/IP.<br>• Sistemas Distribuidos en Web. |
| Título o Certificado | **POST-GRADOS en SISTEMAS DE REDES Y COMUNICACIONES PARA LA SEGURIDAD Y LA DEFENSA.** |

# CERTIFICACIONES PROFESIONALES

| | |
|---|---|
| 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.<br>• 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<br>• Seguridad de las operaciones. Seguridad de los ficheros<br>• 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<br>• Sistemas de autenticación y control de acceso<br>• Seguridad perimetral<br>• Seguridad de las comunicaciones<br>• Seguridad en sistemas operativos<br>• 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<br>• Transición de Servicios TIC. Operación de Servicios TIC<br>• 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.<br>• Conceptos Técnicos sobre la Privacidad.<br>• Reglamentación en ámbitos sectoriales.<br>• 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<br>• Risk Response and Risk Monitoring<br>• IS Control Design and Implementation<br>• 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<br>• Architecture Content Framework<br>• Enterprise Continuum & Tools<br>• Foundation Architecture - TRM and III-RM<br>• 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 Programmes (MSP)<br>• Programme Management: profiles, documentation, processes, activities, and techniques.<br>• Transformational Flow in programmes.<br>• Programme 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 Programmes (MSP).<br>• Theory: Principles and Themes.<br>• Programme 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<br>• Control framework driven by IT Governance.<br>• How COBIT meets the requirement for an IT Governance Framework<br>• How COBIT is used with other standards and best practices<br>• The COBIT Framework and all the components of COBIT<br>• 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.<br>  • 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.<br>• Gestión de Configuración y Cambios. Gestión de Versiones.<br>• Gestión de la Disponibilidad, Continuidad y la Capacidad.<br>• Administración y Estimación Financiera.<br>• 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<br>• Value Delivery<br>• Risk Management and Resource Management<br>• 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)<br>• Los Componentes y los Roles en Gestión de Proyectos PRINCE2<br>• Herramientas y Técnicas en Gestión de Proyectos PRINCE2<br>• 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<br>• Gestión del Riesgo<br>• Gestión del Programa de Seguridad de la Información<br>• Gestión de la Seguridad de la Información<br>• 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<br>• IT Governance<br>• Administración del Ciclo de Vida de Sistemas y de la Infraestructura<br>• Entrega de Servicio y Soporte de TI<br>• Protección de los Activos de Información<br>• 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.<br>• Administración de Configuración, Versiones y Cambios.<br>• Administración de Problemas.<br>• Administración de Disponibilidad, Capacidad y Continuidad.<br>• 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.<br>• SGSI UNE 71502 / BS7799-2.<br>• Análisis de Riesgos.<br>• Planes de Continuidad. |
| Título o Certificado | **EXPERTO EN IMPLANTACIÓN DE SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.** |

## CURSOS SOBRE SEGURIDAD Y DEFENSA

| | |
|---|---|
| Fecha (desde – a) | MARZO 2015 A ENERO 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).<br>○ **Seguridad fronteriza.** Información general y principios generales del espacio Schengen. NATO Joint Advanced Distributed Learning System (NATO JADL).<br>○ **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 Defense 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 ENERO 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 | o **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).<br>o **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), así como a sus misiones operativas actuales. Centro de guerra conjunta de la 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.<br>• 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 2018 |
| 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).<br>□ Arquitectura y Comunicaciones SAP. (LMDATA, 20 Horas)<br>□ Servicios de Directorio y Metadirectorio. CRITICAL PATH CERTIFICATION.<br>□ Servicios Web y Arquitectura SOA. ARTIX. (IONA, 20 Horas).<br>□ Calidad en el Desarrollo del Software (ESPELSA-STC, 100 Horas).<br>□ Bases de Datos Orientadas a Objetos (Ideal Objects S.A, 25 Horas).<br>□ Desarrollo Avanzado de Aplicaciones en Internet (ABS, 50 horas). |

- Programación en Java (LEGIONET – CENTRISA, 40 Horas).
- Arquitectura SIGLO: Cobol CICS DB2, Foundation (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 | A1 |

# ACTIVIDAD INVESTIGADORA

## 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 on a lean methodology with little impact on the organization, suitable for small projects, which reduces start-up time. Software 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, June 12–16, 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.

---

16. J. R. Coz, E Fojón, A. Hernández y G. Colom. ***"Cyber cells: a tool for national cyber security and cyber defence".*** *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.

---

17. 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.

18. 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.

---

19. 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.

---

20. 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.

---

21. 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, la experiencia estoniana y la forma en la que se podrían articular si se consideran interesantes para la política exterior y la ciberseguridad de un país.

---

22. 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 y proyectos de gran alcance que conllevan su desarrollo.

---

23. 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.

---

24. 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.

---

25. 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.

---

26. 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.

---

27. 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€.

---

28. 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.

---

29. 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.

---

30. 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.

31. 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.

---

32. 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.

---

33. 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.

---

34. 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.

---

35. 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.

---

36. 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.

---

37. 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.

---

38. 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.

39. 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.

# PONENCIAS EN CONFERENCIAS Y CONGRESOS

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 grandes sistemas de información 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, 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.

---

8. 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.

---

9. 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 Ejercito 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.

---

10. 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.

---

## LIBROS Y CAPÍTULOS DE LIBROS

(en orden cronológico inverso)

**1. Nuevos Modelos de Analisis 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

---

**2. 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

---

**3. 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), así como la alineación con las expectativas externas.
http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/data-privacy-audit-program.aspx

---

**4. 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

---

**5. 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

---

**6. 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/

---

**7. 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

---

**8. 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

---

**9. 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 de la empresa.
http://www.isaca.org/COBIT/Pages/COBIT-5-spanish.aspx

---

**10. 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

---

**11. 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

---

**12. 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. Febrero 2011.
http://e-spacio.uned.es/fez/eserv.php?pid=tesisuned:IngInf-Jrcoz&dsID=Documento.pdf

---

**13. 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

---

**14. 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

---

**15. 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 de información.
http://www.revistasic.com/revista87/otrostitulos_87.htm

---

**16. 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

---

# 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).

# ENLACES SOBRE ACTIVIDAD CIENTÍFICA E INVESTIGADORA

- Perfil en RESARCH GATE
- Perfil en GOOGLE ACADEMICO
- Perfil en LINKEDIN
- 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 Ejercito 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.

- Nuevo espacio de educación superior en ciberdefensa en el ámbito internacional. Revista SIC. Junio 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 Cibercomandos y la Segregación de Funciones. Real Instituto Elcano. Junio 2015. URL.
- ISAC como nexo 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 puesta 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 Forum 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 defence. 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
- Mesa Redonda del Congreso ENISE 2011 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. LEON, abril 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.
- EFL. Exemplar Flexibilitation Language. Implementación en Ruby. URL
- Desarrollo de familias de productos de software desde un enfoque generativo. URL
- Espacio web de trabajo colaborativo sobre Líneas de Productos Software. URL
- Electronic Notes in Theoretical Computer Science, Volume 238, Number 2, June 2009. URL
- Code Generation with the Exemplar Flexibilitation Language. 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
- Blog con noticias sobre Tecnología y Ciberseguridad. URL

# OTROS DATOS DE INTERES

- Investigador en el Departamento de Economia Aplicada VI de la Universidad Complutense de Madrid. URL
- Profesor Asociado en la Escuela de Negocios Internacional IIBS. URL
- Profesor en la Asociación Española de Auditores de Sistemas (ASIA), en la Universidad Politécnica de Madrid y en la Universidad Europea. URL ISACA. URL UPM. URL UEM.
- Revisor de algunas Revistas 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 o Asian Journal of Research in Computer Science.
- Miembro del Comité Editorial de la Revisita de Investigacion Asian Journal of Applied Science and Technology (AJAST) (ISSN: 2456-883X) URL
- Miembro del Grupo de Investigación de Ingeniería del Software en el Departamento de Ingeniería del Software y Sistemas de la UNED. URL
- Colaborador en las Comisiones de Trabajo de la Asociación Española de Auditores de Sistemas y Responsable del Grupo COBIT PAM. URL
- 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. URL
- Miembro de ISACA. URL
- Miembro Fundador de THIBER, Think Tank sobre Ciberseguridad. URL
- Miembro de la International Input-Output Association (IIOA). URL
- Miembro del Club Internacional BPM. URL
- 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) o la revista Journal of Advances in Mathematics and Computer Science (URL).
- Summary Version of the Curriculum
- Curriculum en INGLES
- Curriculum Versión Reducida