II CONGRESO NACIONAL DE INTEROPERABILIDAD Y SEGURIDAD

"Una Administración más segura y conectada"

Fábrica Nacional de Moneda y Timbre, Madrid, 22 y 23 de febrero de 2012

II CONGRESO NACIONAL DE INTEROPERABILIDAD Y SEGURIDAD:

"Una administración más segura y conectada"

Organiza:

Club de Innovación

Con el apoyo de:

GOBIERNO DE ESPAÑA
MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS

FEMP
FEDERACION ESPAÑOLA DE MUNICIPIOS Y PROVINCIAS

Real Casa de la Moneda
Fábrica Nacional de Moneda y Timbre

GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

CCN
CENTRO CRIPTOLÓGICO NACIONAL

Instituciones colaboradoras:

INTECO
Instituto Nacional de Tecnologías de la Comunicación

IEEE TECHNOLOGY MANAGEMENT COUNCIL

FUNDACIÓN Astic

COSITAL
Secretarios, Interventores y Tesoreros de Administración Local

CNIS 2012

• Miguel A. de Bas
DIRECTOR DE CNIS 2012

• Virginia Moreno
RESPONSABLE DE PROGRAMA

• Virginia Pérez-Bedmar
RESPONSABLE DE ORGANIZACIÓN

• María Gª-Monteavaro
RESPONSABLE DE MARKETING/WEB

Con la colaboración de:

POP SPAIN (Imagen y diseño)

MARIANO&ISABEL (Catering)

ESCUCHA (Audiovisuales)

INFRENT ESPAÑA (Azafatas y merchandising)
TELEVEO.COM (Grabación)

Bienvenidos a la Experiencia CNIS 2012

Un año más nos reunimos para seguir avanzando en la aplicación de los Esquemas Nacionales en nuestras Administraciones Públicas.
Una oportunidad de conocer, de contar y de poner en común las experiencias de dos años de evolución de unas normas que están revolucionando y mejorando la forma de trabajar y de ofrecer los servicios a los ciudadanos.

Quiero en primer lugar agradecer a los asistentes su confianza, nuevamente, en este evento que ya es la referencia para entender y avanzar en los Esquemas Nacionales. Agradecimiento una vez más al Ministerio de Hacienda y Administraciones Públicas, a la Federación Española de Municipios y Provincias y a la Fábrica Nacional de Moneda y Timbre por su apoyo y confianza que este año hemos ampliado con el Ministerio de Industria, Energía y Turismo y el Centro Criptológico Nacional CCN. CERT. Con su apoyo hemos lanzado la nueva convocatoria que esperamos mantener en los próximos años hasta que se haga plenamente realidad "una administración más segura y conectada". Asimismo agradecer la participación activa de los patrocinadores y colaboradores que se han sumado en esta edición a la convocatoria para compartir su experiencia y propuestas, Telefónica, GTT, Gesconsultor, Tecnocom, Blackberry, Banco Santander, Vortal e Indra y también a Ingenia, T-Systems, NAE, Deloitte, Yerbabuena, Mimacom, MDtel, Bilbomática y SoftwareAG.

Además hemos contado con el apoyo de instituciones que están de una u otra forma implicadas en esta materia como el INTECO, el IEEE capítulo español, la Fundación ASTIC y el Cosital.

Este apoyo de todos es para Club de Innovación un aliciente fundamental para seguir en su labor de trabajar "por y para las Administraciones Públicas" animándonos a lanzar nuevos proyectos que anunciaremos en este Congreso CNIS.

Bienvenidos pues a esta experiencia de interrelación entre aquellos que tenéis la inquietud por la innovación y la modernización de las administraciones a las que servís y de aquellos que desde la empresa, aportáis soluciones y hacéis posible el desarrollo de nuestras administraciones.

PROGRAMACIÓN

II CONGRESO NACIONAL DE INTEROPERABILIDAD Y SEGURIDAD
CNIS 2012

MIÉRCOLES, 22 DE FEBRERO DE 2012

8:30 a 9:30h Recepción de asistentes, acreditación y entrega de documentación e invitaciones

SESIONES PLENARIAS - AUDITORIO PRINCIPAL

ESQUEMAS NACIONALES

9:30h INAUGURACIÓN OFICIAL CONGRESO

Intervienen:
D. Aitor Cubo Contreras
Dirección General de Modernización administrativa, procedimientos e impulso de la administración electrónica
Ministerio de Hacienda y Administraciones Públicas

D. Eduardo Javier Contreras Linares
Vicepresidente de la Comisión de NNTT de la FEMP
Alcalde de Molina de Segura

D. David Pérez García
Presidente de la Federación Madrileña de Municipios - FMM
Alcalde de Alcorcón

D. Jaime Sánchez Revenga
Presidente - Director General FNMT

D. Miguel Ángel de Bas Sotelo
Director Club de Innovación

10:00h "MODERNIZACIÓN ADMINISTRATIVA, PROCEDIMIENTOS E IMPULSO DE LA ADMINISTRACIÓN ELECTRÓNICA. Aplicando los Esquemas Nacionales"

D. Aitor Cubo Contreras
Dirección General de Modernización administrativa, procedimientos e impulso de la administración electrónica
Ministerio de Hacienda y Administraciones Públicas

10:15h Coloquio "MODERNIZACION DE LAS CIUDADES A TRAVÉS DE LAS TICS. Una apuesta necesaria"

Modera:
Dª Trinidad Yera Cuesta
Directora General de Gestión de Políticas Locales
FEMP

Participan:
D. David Pérez García
Presidente de la Federación Madrileña de Municipios - FMM
Alcalde de Alcorcón

D. Eduardo Javier Contreras Linares
Vicepresidente de la Comisión de NNTT de la FEMP
Alcalde de Molina de Segura

D. Antonio Jesús Ruiz Aguilar
Vocal de la Comisión de NNTT de la FEMP
Teniente Alcalde de Vivienda del Ayuntamiento de El Puerto de Santa María

D. Eduardo Villanueva Bayona
Concejal de Modernización y Nuevas Tecnologías
Ayuntamiento de Burgos

11:00 a 11:30h Pausa, Café

SESIONES PLENARIAS - AUDITORIO PRINCIPAL

INTEROPERABILIDAD

11:30h "REUTILIZACIÓN DE APLICACIONES. CENTRO DE TRANSFERENCIA DE TECNOLOGÍA - CTT, EL CASO DE ACCEDA."

D. Carlos Marcos Martín
Dirección General de Modernización administrativa, procedimientos e impulso de la administración electrónica.
Ministerio de Hacienda y Administraciones Públicas

11:50h "INTEROPERABILIDAD EN LA SMART CITY"

D. Jose Luis Nuñez Freile
Desarrollo de Negocio. Ingenieria M2M y Soluciones Sectoriales
Telefónica

D. José Carlos Sendra Alcina
M2M Services
Telefónica Investigación y Desarrollo

12:10h "INTEROPERABILIDAD Y SEGURIDAD. La visión de la Comisión Europea"

D. Jorge Remuiñán Suárez
Programme Manager
Dirección General de Informática
Comisión Europea

"LA INTEROPERABILIDAD TRANSFRONTERIZA COMO CLAVE DE FUTURO"

D. Carlos E. Jiménez
Proyecto e-Justicia.cat del Departamento de Justicia de la Generalitat de Catalunya
Redactor del Marco Iberoamericano de Interoperabilidad
Presidente del capítulo español del IEEE TMC

12:40h "APLICANDO LAS NORMAS TÉCNICAS DE INTEROPERABILIDAD, EL CASO DE SIR Y ORVE"

D. Miguel Ángel Amutio Gómez
Jefe de Área de Planificación y Explotación
Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica
Ministerio de Hacienda y Administraciones Públicas

12:55h Coloquio-Debate: "EN EL ECUADOR DE LA ADECUACIÓN A LOS ESQUEMAS NACIONALES ¿Dónde estamos?"

Modera:
D. Mario Alguacil Sanz
Director Tecnologías y Gestión del Conocimiento
Ayuntamiento de Sant Feliu de Llobregat

Participan:
D. Josep Monterde
Cap d'Innovació, processos i qualitat
Ayuntamiento de Terrasa

D. Victor Manuel Solla Bárcerna
Jefe de Servicio de Sistemas de Información
Ayuntamiento de Avilés

D. Antonio López-Fuensalida Sánchez-Paulete
Representante de informática
Ayuntamiento de Madrid

D. Claudio Pérez-Olea Meyer-Döhner
Subdirector General de Programas de Atención al Ciudadano
Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica.
Secretaría de Estado de Administraciones Públicas
Ministerio de Hacienda y Administraciones Públicas

13:30h Caso práctico: "LA INTEROPERABILIDAD A TRAVÉS DE LA PALS (Plataforma Avanza Local Soluciones)"

Dª. María Tránsito Jaroso Blanco
Consejera técnica. Responsable de las aplicaciones Efacil, Padrón y Lopd de la
Plataforma Avanza Local Soluciones

Dª Silvia Vicente del Hoyo
Jefe de área técnica. Responsable de las aplicaciones SIGM, LocalGIS y Localweb de la
Plataforma Avanza Local Soluciones.
Ministerio de Industria, Energía y Turismo

13:50h Caso práctico: "MODULO INE DE INTERCAMBIO DE DATOS CON EL PADRON DE HABITANTES"

D. José Luis Maldonado
Instituto Nacional de Estadística

14:10h Caso Práctico: "PLATAFORMA DE INTERMEDIACIÓN: SERVICIOS DE VERIFICACIÓN Y CONSULTA DE DATOS"

Presenta:
Dª. Montaña Merchán Arribas
Directora de la División de Proyectos de Administración Electrónica.
Dirección General para el Impulso de la Administración Electrónica
Ministerio de Hacienda y Administraciones Públicas

Expone:
D. José Antonio Eusamio
Jefe de área de Planificación y Proyectos Tecnológicos
División de Proyectos de Administración Electrónica
Ministerio de Hacienda y Administraciones Públicas

14:35 a 16:00h Almuerzo

16:00h Coloquio-Debate: "LA INTEROPERABILIDAD TAMBIÉN EN LA GESTIÓN DE TRIBUTOS. Y el ahorro tangible en costes"

Modera:
D. Manuel Mendieta
Director Comercial
GTT

Participan:
Dª. Carmen Conejo
Subdirectora General adjunta de Estudios y sistemas de información.
D.G del Catastro.
Ministerio de hacienda y Administraciones Públicas

D. Luis de Eusebio

Subdirección General de Informática
Dirección General de Tráfico

D. Mario Abascal
Director General
Agencia Notarial de Certificación ANCERT

D. Ramón Ferri
Jefe de Servicio TIC. Servicio de Tecnología de la Innovación
Ayuntamiento de Valencia

D. Enrique Calvete
Tesorero
Diputación de A Coruña

16:50h "SISTEMA DE GESTIÓN DOCUMENTAL DE TRÁFICO. Un modelo operativo de la Interoperabilidad del documento y expediente electrónico"

D. Alfonso Berral
Jefe de Servicio de Sistemas Informáticos
Subdirección General de Informática
Dirección General de Tráfico

17:10h Coloquio-Debate: "DISTINTAS VISIONES DE LA INTEROPERABILIDAD ¿Entendemos todos lo mismo?"

Modera:
D. Diego Hernández
Director Ceres
FNMT

Participan:
D. Carlos Marcos Martín
Dirección General de Modernización administrativa, procedimientos e impulso de la administración electrónica.
Ministerio de Hacienda y Administraciones Públicas

D. Larry Bensadon
Director Desarrollo de Negocio
BlackBerry

D. Fernando Marina
Jefe del Servicio de Informática
Diputación Provincial de Málaga

D. Roberto Santos Santos
Interoperabilidad y Software libre
Marketing Sector AA.PP
Telefónica Grandes Clientes

18:00h "Y EN SANIDAD… LA INTEROPERABILIDAD"

Dª. Zaida Sampedro
Directora General de Sistemas de Información Sanitaria
SERMAS
Consejería de Sanidad de la Comunidad de Madrid

18:20h CONCLUSIONES PRIMERA JORNADA DE TRABAJO

Presenta:
Dª. Virginia Moreno Bonilla
Consultora de administración pública
Asesora en modernización, simplificación y e-administración
Especializada en temas locales
Entrega encuestas de calidad 1ª jornada

18:30h SORTEO

18:40h FIN JORNADA DE TRABAJO

MIÉRCOLES, 22 DE FEBRERO DE 2012

SALA DE COMUNICACIONES

SEGURIDAD

11:00 a 11:30h Café

11:30h "IMPLANTACIÓN DEL ENS EN LA PRÁCTICA"

D. Juan Crespo Sánchez
Inspector Jefe
Área de Informática
Cuerpo Nacional de Policía

D. Diego López Román
Responsable Desarrollo de Negocio de Infraestructuras
Dirección de Marketing de Infraestructuras
Telefónica

12:00h "RESPONSABILIDAD Y PROTECCIÓN DEL DATO, VISIÓN PRAGMÁTICA DE SOLUCIÓN. PROCESOS, CONCIENCIACIÓN Y MECANISMOS DE SECURIZACIÓN NECESARIOS".

D. Israel Córdoba
Director de desarrollo de Negocio. División Seguridad
MDtel

12:30h "INTEGRACIÓN DEL ENS CON EL SGSI EN LA CONSEJERÍA DE CULTURA DE LA JUNTA DE ANDALUCÍA: la plataforma "e-PULPO" como herramienta de gestión global"

Dª. Elísa García
Consultora de Seguridad Estratégica
INGENIA

13:00h "GESTIÓN T.I., RIESGO Y CUMPLIMIENTO DEL E.N.S. Visión práctica completa de una AA.PP. utilizando GESCONSULTOR, OSSIM-ALIENVAULT y PILAR de forma integrada"

D. Óscar Bou Bou
Auditor Jefe de Certificación de S.G.S.I.s (ISO 27001
Responsable de Producto
GESCONSULTOR

D. Victorino Martín Jorcano
Director de Operaciones. ALIENVAULT creators of ossim

13:30h "LICITACIÓN PÚBLICA ELECTRÓNICA. Presente y Futuro de la contratación"

D. José Luis Arístegui
Gerente administración Pública
Vortal Conecting Services

14:00h "GESTIÓN INTEGRAL DEL CUMPLIMIENTO: ESQUEMA NACIONAL DE SEGURIDAD"

D. Luis Carro
Socio del Área de Riesgos Tecnológicos de Deloitte

14:30 a 16:00h Almuerzo

16:00h EL PORTAL DE LAS ENTIDADES LOCALES

Dª Nimia Rodriguez Escolar
División de Sistemas de la Información y Comunicaciones
Ministerio de Hacienda y Administraciones Públicas

16:30h "NO SIN MI BlackBerry"

D. Larry Bensadon
Director Desarrollo de Negocio

Dª. Chelo Albarca
Directora Relaciones Institucionales
BlackBerry

17:00h "ACTUACIONES Y NUEVAS INICIATIVAS DE LAS COMISIONES DE TRABAJO DE LA FEMP"

D. Pablo Bárcenas
FEMP

17:30h "CUMPLIMIENTO DEL ENS DESDE EL PUNTO DE VISTA DEL PROVEEDOR. El caso Telefónica".

D. Jose Luis Vega Prada
Jefe de Procesos y certificación. Dirección de Atención al cliente y Gestión comercial
Telefónica

D. Luis Molina Borao
Director Asociado
NAE

18:00h ADECUACIÓN DE 368 AYUNTAMIENTOS DE LA PROVINCIA DE BURGOS MENORES DE 10.000 HABITANTES AL ESQUEMA NACIONAL DE SEGURIDAD (ENS) SEMANTIC – DIPUTACIÓN DE BURGOS

D. Javier Peña Alonso
Modernización Administrativa y Nuevas Tecnologías de la Información y las Comunicaciones
Diputación de Burgos

18:20h Fin de las comunicaciones de Seguridad.
Conclusiones y sorteo en el Auditorio

JUEVES, 23 DE FEBRERO DE 2012

9:00 a 9:30h Recepción de asistentes, acreditaciones y entrega de documentación

SESIONES PLENARIAS - AUDITORIO PRINCIPAL

SEGURIDAD

9:30h "CÓMO SE HA EVOLUCIONADO DESPUÉS DE UN AÑO EN EL ENS. ¿Qué se les ofrece a las Administraciones?"
D. Miguel A. Amutio

Jefe de Área de Planificación y Explotación
Ministerio de Hacienda y Administraciones Publicas

D. Javier Candau
Jefe del Área de Políticas y Servicios
Centro Criptológico Nacional CCN-CERT

09:50h Coloquio-Debate: "ENFOQUES DE ÉXITO EN PROYECTOS DE ADECUACIÓNAL ESQUEMA NACIONAL DE SEGURIDAD"

Modera:
D. Oscar Bou Bou
Auditor Jefe de Certificación de S.G.S.I.s (ISO 27001).
Responsable de Producto "Gesconsultor"

Participan:
D. Eusebio Moya López
Responsable de Seguridad de Sistemas de Información
Diputación de Valencia

D. José Francisco Hidalgo Céspedes
Responsable Seguridad y Certificación
Universidad de Murcia

D. Adrián Ballester Espinosa
Diputado de Modernización
Diputación de Alicante

D. Alberto López
Gerente de proyectos
INTECO

10:40h Coloquio-Debate: "SEGURIDAD Y SERVICIOS CLOUD. Mejor alternativa"

Modera:
D. José Benedito Agramunt
Jefe de Servicio de Informática y Organización
Diputación de Valencia

Participan:
D. José Antonio Ñiguez
Director de área técnica
GTT

D. Alfonso José Martín Palma
Gerente Responsable de Soluciones de Ciberseguridad
INDRA SISTEMAS, S.A.

Dª. Montaña Merchán Arribas
Directora de la División de Proyectos de Administración Electrónica.
Dirección General para el Impulso de la Administración Electrónica
Ministerio de Hacienda y Administraciones Públicas

D. Juan Crespo
Inspector Jefe
Área de Informática
Cuerpo Nacional de Policía

D. Josep Clotet Sopeña
Gerente del Parque Científico y Tecnológico Agroalimentario de Lleida
Coordinador de la Comisión de Trabajo y del Grupo Técnico de Sociedad de la Información y Nuevas Tecnologías, de la Federación Española de Municipios y Provincias

11:30 a 12:00h Pausa, Café

12:00h Coloquio-Debate: "CLOUD Y AHORRO DE COSTES: LICITACIÓN PÚBLICA ELECTRÓNICA. Interoperabilidad segura también con los Proveedores"

Modera:
D. Carlos Galán
Profesor
Universidad Carlos III

Participan:
Dª. Almudena Moreno
Gerente
Caiber

D. Javier Peña
Modernización Administrativa y Nuevas Tecnologías de la Información y las Comunicaciones
Diputación de Burgos

Dr. Artur Trindade Mimoso
Director Unidad Ministerial de Compra Centralizada
Ministerio de Defensa de Portugal

D. José Francisco Garrido
Jefe de Compras
FNMT

12:50h "BYOD; Bring your own device" (trae tu propio dispositivo)

D. Larry Bensadon
Director Desarrollo de Negocio
BlackBerry

13:10h "GESTIÓN ELECTRÓNICA DE EXPEDIENTES"

D. Aitor Cubo Contreras
Dirección General de Modernización administrativa, procedimientos e impulso de la administración electrónica
Ministerio de Hacienda y Administraciones Públicas

13:30h "SEGURIDAD. Vision desde la red"

D. Diego López Román
Responsable Desarrollo de Negocio de Infraestructuras
Dirección de Marketing de Infraestructuras
Telefónica

13:50h Coloquio-Debate: "EL PAPEL CLAVE DE LA GESTIÓN DOCUMENTAL"

Modera:
D. Alfonso Díaz
Archivero
Principado de Asturias

Participan:
Dña. Sonia Crespo
Archivera Municipal
Ayuntamiento de Rivas-Vaciamadrid

D. Fernando Marina
Jefe del servicio de Informática
Diputación Provincial de Málaga

D. Carlos Castro
Gerente Desarrollo de Negocio
Tecnocom

D. Alfonso Berral
Jefe de Servicio de Sistemas Informáticos
Subdirección General de Informática
Dirección General de Tráfico

14:40 a 16:00h Almuerzo

16:00h Coloquio-Debate: "HABILITADOS NACIONALES QUE APUESTAN POR EL ENS EN LA ADMINISTRACIÓN. Después de 1 año, ¿siguen apostando?

Modera:
D. Manuel Serrano
Jefe del Servicio de Calidad y Modernización
Ayuntamiento de Málaga

Participan:
D. Eulalio Ávila Cano
Secretario Ayuntamiento de Majadahonda.
Presidente Cosital

D. José Félix Rodríguez Busto
Tesorero Diputación Provincial de Burgos

D. Rafael Salgado Gimeno
Vice secretario General Ayuntamiento de Valladolid

D. Vicente Calvo y del Castillo
Interventor Ayuntamiento de Ferrol

17:00h Solución a dudas: "TENGO UNA PREGUNTA PARA USTED: Marco y modelo jurídico en el que nos movemos"

Dª. Ana Marzo
D. Carlos Galán
Abogados especialistas en tecnología

17:30h CONCLUSIONES SEGUNDA JORNADA

Presenta:
Dª. Virginia Moreno Bonilla
Consultora de administración pública
Asesora en modernización, simplificación y e-administración
Especializada en temas locales

17:45h ACTO DE ENTREGA DE PREMIOS CNIS - MEJORES PRÁCTICAS EN ADMINISTRACIÓN PÚBLICA Y PRIVADA
Acto patrocinado por BANCO SANTANDER

1. *Premio proyecto referente en Interoperabilidad y/o Seguridad en Administración Central*

2. *Premio proyecto referente en Interoperabilidad y/o Seguridad en Administración Autonómica*

3. *Premio proyecto referente en Interoperabilidad y/o Seguridad en Diputaciones*

4. *Premio proyecto referente en Interoperabilidad y/o Seguridad en Administración Local*

5. *Premio proyecto referente en Administración Electrónica por su adecuación a la normativa Vigente*

6. *Premio a su Trayectoria Profesional por su implicación en el desarrollo y cumplimiento de los EENN y el empeño profesional en la administración pública*

7. *Premio al compromiso con lo público*

8. *Mención Especial: Colaboración en divulgación y actualización de información a favor de las administraciones públicas, en los EENN*

Entrega de premios por FEMP, FNMT, Ministerios, Fundaciones y Patrocinadores, promovidos por Club de Innovación

18:15h CLAUSURA

Entrega encuestas de calidad 2ª jornada

18:20h SORTEO

18:30h FIN DEL CONGRESO

JUEVES, 23 DE FEBRERO DE 2011

SALA DE COMUNICACIONES

INTEROPERABILIDAD

9:30h "MÓDULOS DE INTEROPERABILIDAD INE Y MINISTERIO DE INDUSTRIA, ENERGIA Y TURISMO"

Dª. María Tránsito Jaroso Blanco
Consejera técnica. Responsable de las aplicaciones Efacil, Padrón y Lopd de la Plataforma Avanza Local Soluciones

Dª. Silvia Vicente del Hoyo
Jefe de área técnica. Responsable de las aplicaciones SIGM, LocalGIS y Localweb de la Plataforma Avanza Local Soluciones.
Ministerio de Industria, Energía y Turismo

D. José Luis Maldonado
Subdirección General de Tecnologías de la Información y de las comunicaciones
Instituto Nacional de Estadística

"EL PAPEL DE SOFTWARE AG EN EL NUEVO MODELO DE GESTIÓN INTEGRADA DE POBLACIÓN Y TERRITORIO"

D. Javier Sambade
Gerente de Administración Pública de Global Consulting
SOFTWARE AG

10:30 h "EL APAGÓN DEL PAPEL Y EL ENI: EL SISTEMA DE INTERCONEXIÓN DE REGISTROS"

D. Claudio Pérez-Olea Meyer-Döhner
Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica. Ministerio de Hacienda y Administraciones Públicas

10.50h "Visión técnica de la reutilización de productos y servicios"

D. Enrique Caballero
Account Manager
Bilbomática

11:00h "4 CLAVES PARA ADAPTAR MI ADMINISTRACIÓN AL ENI"

D. Rubén Lirio
Director Ventas
Yerbabuena Software

11:30 a 12:00h Pausa, Café

12:00h "CASO PRACTICO APLICACIÓN: FOLIADO ELECTRÓNICO, VISTA ELECTRÓNICA, PUESTA A DISPOSICIÓN Y REMISIÓN DEL EXPEDIENTE ELECTRÓNICO"

D. Juan Manuel Gómez Acín
Responsable Unidad "Economía y Hacienda" de la B.U. TAO de T-Systems
T-Systems

12:30h "LA INTEROPERABILIDAD Y EL EXPEDIENTE ELECTRÓNICO"

D. Emilio Gonzalez Cancelo
Magister en Administración Electrónica
INDRA SISTEMAS, S.A.

13:00h "CUANTO CUESTA ADAPTARSE AL ENI"

D. Julio Espiña
Gerente
TECNOCOM

13:30h "INTEROPERABILIDAD Y OPEN DATA"

D. Guillermo Conde Heredia
e-Administracion
Telefónica Grandes Clientes

D. Francisco Javier Tur Cano
Soluciones de Internet
Telefónica Grandes Clientes

14:00h "TangramBPM:la plataforma para la interoperabilidad".

D. Domingo Laborda
Director de Consultoría
mimacom

14:30 a 16:00h Almuerzo

16:00h "ENS-EÑANDO Y ENI-CIANDO EL CUMPLIMIENTO DE LOS ESQUEMAS EN LOS AYUNTAMIENTOS DE LA PROVINCIA DE BARCELONA"

Dª Magda Lorente Martínez
Jefa de la Sección de Asistencia en Sistemas de Información Local
D. Joan Carles Batalla Edo
Jefe de la Sección de Asistencia en Nuevas Tecnologías

D. José Antonio Arranz de Gracia
Responsable de las líneas de asistencia en Protección de Datos y Seguridad
Oficina d'Assistència en Administració Electrònica
Diputación de Barcelona

16:30h "LA INTEROPERABILIDAD COMO PROYECTO DE INNOVACIÓN. El presente en la Administración de la Comunidad de Castilla y León".

Dª. Isabel Valle de Juana
Direcctora General de Atención al Ciudadano, Calidad y Modernización.
Junta de Castilla y León

17:30h Fin de las comunicaciones de Interoperabilidad.

Conclusiones Entrega de Premios CNIS 2012, Clausura y sorteo en el Auditorio

NORMAS TÉCNICAS DE INTEROPERABILIDAD

El Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica establece, en su disposición adicional primera, el desarrollo de la serie de ***Normas Técnicas de Interoperabilidad*** que son de obligado cumplimiento por parte de todas las Administraciones Públicas.

Las Normas Técnicas de Interoperabilidad desarrollan cuestiones concretas para asegurar los aspectos más prácticos y operativos de la interoperabilidad entre las Administraciones Públicas, entre sí y con los ciudadanos, profesionales y empresas.

Seguidamente, se hace un breve resumen del contenido de aquellas Normas Técnicas que, a fecha de redacción de este documento, han sido publicadas.

Resolución de 19 de julio de 2011, de la Secretaría de Estado para la Función Pública, por la que se aprueba la Norma Técnica de Interoperabilidad de:

DIGITALIZACIÓN DE DOCUMENTOS.

Fecha de publicación: 30 de julio de 2011
BOE núm. 182 / Sec. III / Pág. 87091
http://www.boe.es/boe/dias/2011/07/30/pdfs/BOE-A-2011-13168.pdf

La Norma Técnica de Interoperabilidad de Digitalización de Documentos establece los ***componentes de un documento electrónico digitalizado***, incluyendo la imagen electrónica, firma electrónica y metadatos, así como las ***reglas para la digitalización de documentos en soporte papel*** por parte de las Administraciones públicas, atendiendo a los formatos, niveles de calidad, condiciones técnicas y estándares aplicables; y para los aspectos relativos a la gestión y conservación de los documentos electrónicos digitalizados se remite a la Norma Técnica de Interoperabilidad de Política de Gestión de Documentos Electrónicos.

Índice.

I. Objeto.
II. Ámbito de aplicación.
III. Documentos electrónicos digitalizados.
IV. Requisitos de la imagen electrónica.
V. Proceso de digitalización.

Guía de aplicación de la Norma Técnica de Interoperabilidad de Digitalización de Documentos.

http://www.mpt.gob.es/dms/es/publicaciones/centro_de_publicaciones_de_la_sgt/GUIAS_NTI/text_es_files/Guia_digitaliz-documentos-INTERNET.pdf

Resolución de 19 de julio de 2011, de la Secretaría de Estado para la Función Pública, por la que se aprueba la Norma Técnica de Interoperabilidad de:

DOCUMENTO ELECTRÓNICO.

Fecha de publicación: 30 de julio de 2011
BOE núm. 182 / Sec. III / Pág. 87094
http://www.boe.es/boe/dias/2011/07/30/pdfs/BOE-A-2011-13169.pdf

La Norma Técnica de Interoperabilidad de Documento electrónico ***establece los componentes del documento electrónico***, incluyendo contenido, firma electrónica y metadatos mínimos obligatorios, y su formato, así como las condiciones para su intercambio y reproducción; para los aspectos relativos a la gestión y conservación de los documentos electrónicos se remite a la Norma Técnica de Interoperabilidad de Política de gestión de documentos electrónicos.

Finalmente, se incluye en anexo la definición detallada de los ***metadatos mínimos obligatorios, los esquemas XML para intercambio de documentos y la información básica de firma de documentos electrónicos***. En este sentido, la estructura de documento electrónico definida en esta norma permite la utilización de las firmas electrónicas contempladas en la Decisión de la Comisión 2011/130/EU de 25 de febrero de 2011 por la que se establecen los requisitos mínimos para el tratamiento transfronterizo de los documentos firmados electrónicamente por las autoridades competentes en virtud de la Directiva 2006/123/CE del Parlamento Europeo y del Consejo relativa a los servicios en el mercado interior.

Índice

I. Objeto.
II. Ámbito de aplicación.
III. Componentes del documento electrónico.
IV. Firma del documento electrónico.
V. Metadatos del documento electrónico.
VI. Formato de documentos electrónicos.
VII. Intercambio de documentos electrónicos.
VIII. Acceso a documentos electrónicos.
Anexo I. Metadatos mínimos obligatorios del documento electrónico.
Anexo II. Esquemas XML para intercambio de documentos electrónicos.
Anexo III. Información básica de la firma de documentos electrónicos.

Guía de aplicación de la Norma Técnica de Interoperabilidad de Documento Electrónico.

http://www.mpt.gob.es/dms/es/publicaciones/centro_de_publicaciones_de_la_sgt/GUIAS_NTI/text_es_files/Guia_documento-electronico-INTERNET.pdf

Resolución de 19 de julio de 2011, de la Secretaría de Estado para la Función Pública, por la que se aprueba la Norma Técnica de Interoperabilidad de:

EXPEDIENTE ELECTRÓNICO.

Fecha de publicación: 30 de julio de 2011
BOE núm. 182 / Sec. III / Pág. 87108
http://www.boe.es/boe/dias/2011/07/30/pdfs/BOE-A-2011-13170.pdf

La Norma Técnica de Interoperabilidad de Expediente electrónico establece la ***estructura de los expedientes electrónicos***, que incluye documentos electrónicos, índice electrónico, firma electrónica y metadatos mínimos obligatorios, así como las especificaciones para los servicios de remisión y puesta a disposición; para los aspectos relativos a la gestión y conservación de los expedientes electrónicos se remite a la Norma Técnica de Interoperabilidad de Política de gestión de documentos electrónicos.

Finalmente, se incluye en anexo la definición detallada de los ***metadatos mínimos***

obligatorios y los esquemas XML para el intercambio de expedientes electrónicos.
En este sentido, la estructura de expediente electrónico definida en esta norma permite la utilización de las firmas electrónicas contempladas en la Decisión de la Comisión 2011/130/EU, de 25 de febrero de 2011, por la que se establecen los requisitos mínimos para el tratamiento transfronterizo de los documentos firmados electrónicamente por las autoridades competentes en virtud de la Directiva 2006/123/CE del Parlamento Europeo y del Consejo relativa a los servicios en el mercado interior.

Índice
I. Objeto.
II. Ámbito de aplicación.
III. Componentes del expediente electrónico.
IV. Metadatos del expediente electrónico.
V. Intercambio de expedientes electrónicos.
Anexo I. Metadatos mínimos obligatorios del expediente electrónico.
Anexo II. Esquemas XML para intercambio de expedientes electrónicos.

Guía de aplicación de la Norma Técnica de Interoperabilidad de Expediente Electrónico.

http://www.mpt.gob.es/dms/es/publicaciones/centro_de_publicaciones_de_la_sgt/GUIAS_NTI/text_es_files/Guia_expediente-electronico-INTERNET.pdf

Resolución de 19 de julio de 2011, de la Secretaría de Estado para la Función Pública, por la que se aprueba la Norma Técnica de Interoperabilidad de:

POLÍTICA DE FIRMA ELECTRÓNICA Y DE CERTIFICADOS DE LA ADMINISTRACIÓN.

Fecha de publicación: 30 de julio de 2011
BOE núm. 182 / Sec. III / Pág. 87121
http://www.boe.es/boe/dias/2011/07/30/pdfs/BOE-A-2011-13171.pdf

La Norma Técnica de Interoperabilidad de Política de firma electrónica y de certificados de la Administración establece el conjunto de ***criterios para el desarrollo o adopción de políticas de firma electrónica basada en certificados*** por parte de las Administraciones públicas. Para ello, define el ***contenido de una política de firma electrónica*** basada en certificados, especificando las características de las reglas comunes, como formatos, uso de algoritmos, creación y validación de firma para documentos electrónicos, así como de las reglas de confianza en certificados electrónicos, sellos de tiempo y firmas longevas.

Las condiciones establecidas en esta norma pretenden establecer un marco para la definición de políticas de firma electrónica basada en certificados alineada con las últimas tendencias a nivel europeo como es la Decisión de la Comisión 2011/130/EU, de 25 de febrero de 2011, por la que se establecen los requisitos mínimos para el tratamiento transfronterizo de los documentos firmados electrónicamente por las autoridades competentes en virtud de la Directiva 2006/123/CE del Parlamento Europeo y del Consejo relativa a los servicios en el mercado interior, compatible a su vez con sistemas de firma electrónica ya implantados.

Índice
I. Consideraciones generales.
I.1 Objeto.
I.2 Ámbito de aplicación.
II. La política de firma electrónica.
II.1 Definición y contenido.
II.2 Datos identificativos de la política.
II.3 Actores involucrados en la firma electrónica.
II.4 Usos de la firma electrónica.
II.5 Interacción con otras políticas.
II.6 Gestión de la política de firma.
II.7 Archivado y custodia.
III. Reglas comunes.

III.1 Reglas comunes.
III.2 Formatos admitidos de firma electrónica.
III.3 Firma electrónica de transmisiones de datos.
III.4 Firma electrónica de contenido.
III.5 Reglas de uso de algoritmos.
III.6 Reglas de creación de firma electrónica.
III.7 Reglas de validación de firma electrónica.
IV. Reglas de confianza.
IV.1 Reglas de confianza para los certificados electrónicos.
IV.2 Reglas de confianza para sellos electrónicos.
IV.3 Reglas de confianza para firmas longevas.
Anexo. Etiquetas de creación y validación de firmas electrónicas para los formatos admitidos.

Guía de aplicación de la Norma Técnica de Interoperabilidad de Política de Firma Electrónica y de Certificados de la Administración.

http://www.mpt.gob.es/dms/es/publicaciones/centro_de_publicaciones_de_la_sgt/GUIAS_NTI/text_es_files/Guia_politica-firma-elect-certif-admon-INTERNET.pdf

Resolución de 19 de julio de 2011, de la Secretaría de Estado para la Función Pública, por la que se aprueba la Norma Técnica de Interoperabilidad de:

PROCEDIMENTOS DE COPIADO AUTÉNTICO Y CONVERSIÓN ENTRE DOCUMENTOS ELECTRÓNICOS.

Fecha de publicación: 30 de julio de 2011
BOE núm. 182 / Sec. III / Pág. 87134
http://www.boe.es/boe/dias/2011/07/30/pdfs/BOE-A-2011-13172.pdf

La Norma Técnica de Interoperabilidad de Procedimientos de copiado auténtico y conversión entre documentos electrónicos establece las ***reglas para la generación y expedición de copias electrónicas auténticas, copias papel auténticas de documentos públicos administrativos electrónicos y para la conversión de formato de documentos electrónicos*** por parte de las Administraciones públicas; para los aspectos relativos a la gestión de los documentos resultantes del proceso de copiado auténtico o conversión, se remite a la Norma Técnica de Interoperabilidad de Política de gestión de documentos electrónicos.

Índice
I. Objeto.
II. Ámbito de aplicación.
III. Características generales de las copias electrónicas auténticas.
IV. Copia electrónica auténtica con cambio de formato.
V. Copia electrónica auténtica de documentos papel.
VI. Copia electrónica parcial auténtica.
VII. Copia papel auténtica de documentos públicos administrativos electrónicos.
VIII. Conversión entre documentos electrónicos.

Guía de aplicación de la Norma Técnica de Interoperabilidad de Copiado Auténtico y Conversión entre documentos electrónicos.

http://www.mpt.gob.es/dms/es/publicaciones/centro_de_publicaciones_de_la_sgt/GUIAS_NTI/text_es_files/Guia_copiado-conversion-doc-elec-INTERNET.pdf

Resolución de 19 de julio de 2011, de la Secretaría de Estado para la Función Pública, por la que se aprueba la Norma Técnica de Interoperabilidad de:

REQUISITOS DE CONEXIÓN A LA RED DE COMUNICACIONES DE LAS ADMINISTRACIONES PÚBLICAS ESPAÑOLAS.

Fecha de publicación: 30 de julio de 2011
BOE núm. 182 / Sec. III / Pág. 87138
http://www.boe.es/boe/dias/2011/07/30/pdfs/BOE-A-2011-13173.pdf

La Norma Técnica de Interoperabilidad de Requisitos de conexión a la Red de comunicaciones de las Administraciones públicas españolas se desarrolla bajo lo establecido en el artículo 43 de la Ley 11/2007, de 22 de junio, y artículo 13 del Real Decreto 4/2010, de 8 de enero, para ***posibilitar la interconexión de las redes de las Administraciones públicas*** y permitir el intercambio de información entre las mismas, así como la ***interconexión con las redes de las Instituciones de la Unión Europea y de otros Estados Miembros.***

La Norma Técnica de Interoperabilidad de Requisitos de conexión a la Red de comunicaciones de las Administraciones públicas españolas establece las condiciones en las que cualquier órgano de una Administración, o Entidad de Derecho Público vinculada o dependiente de aquélla, accederá a la Red SARA, y describe los ***roles y responsabilidades de los agentes que se conectan a la Red SARA*** así como los requisitos para la conexión, acceso y uso de los servicios que se prestan a través de aquélla.

Índice

I. Consideraciones generales.
I.1 Objeto.
I.2 Ámbito de aplicación.
II. Agentes y conexión a la Red SARA.
II.1 Conexión a la Red SARA.
II.2 MPTAP-Centro de Soporte de la Red SARA.
II.3 Proveedores de Acceso a la Red SARA (PAS).
II.4 Órganos usuarios finales.
III. Requisitos técnicos para la conexión del PAS.
III.1 Esquema del Área de Conexión (AC).
III.2 Administración de la conexión.
III.3 Plan de direccionamiento.
III.4 Dotación de elementos de conectividad.
III.5 Garantías de acondicionamiento físico.
III.6 Servicios de soporte y gestión de incidentes.
IV. Acceso y utilización de servicios.
IV.1 Acceso a los servicios.
IV.2 Mantenimiento del catálogo de servicios.
IV.3 Condiciones de utilización de los servicios.
V. Agentes y roles.
V.1 Ministerio de Política Territorial y Administración Pública.
V.2 Proveedores de acceso a la Red SARA.
V.3 Órganos usuarios finales.
V.4 Publicidad de referencias.

Guía de aplicación de la Norma Técnica de Interoperabilidad de Requisitos de Conexión a la Red de Comunicaciones de las Administraciones Públicas Españolas.

http://www.mpt.gob.es/dms/es/publicaciones/centro_de_publicaciones_de_la_sgt/GUIAS_NTI/text_es_files/Guia_conex-red-AA-PP-esp-INTERNET.pdf

Resolución de 19 de julio de 2011, de la Secretaría de Estado para la Función Pública, por la que se aprueba la Norma Técnica de Interoperabilidad de:

MODELO DE DATOS PARA EL INTERCAMBIO DE ASIENTOS ENTRE LAS ENTIDADES REGISTRALES.

Fecha de publicación: 30 de julio de 2011
BOE núm. 182 / Sec. III / Pág. 87145
http://www.boe.es/boe/dias/2011/07/30/pdfs/BOE-A-2011-13174.pdf

La Norma Técnica de Interoperabilidad de Modelo de Datos para el intercambio de asientos entre las Entidades Registrales responde a lo recogido en el artículo 24.4 de la Ley 11/2007, de 22 de junio, que establece que en el ámbito de la Administración General del Estado se automatizarán las

oficinas de registro físicas a fin de ***garantizar la interconexión de todas sus oficinas y posibilitar el acceso por medios electrónicos a los asientos registrales y a las copias electrónicas de los documentos presentados***, lo que ha promovido, en el marco del Esquema Nacional de Interoperabilidad, la elaboración una nueva versión de la norma de intercambio registral, ***SICRES (Sistema de Información Común de Registros de Entrada y Salida)***, para normalizar la interoperabilidad entre las distintas oficinas de registro. Asimismo, la norma extiende esta interoperabilidad a los registros electrónicos de las diferentes Administraciones y sus especificaciones se apoyan en el desarrollo del resto de Normas Técnicas de Interoperabilidad previstas en el Real Decreto 4/2010, de 8 de enero, y en particular, en el cumplimiento del artículo 9 del mismo.

La finalidad principal de la Norma Técnica de Interoperabilidad de Modelo de Datos para el intercambio de asientos entre las Entidades Registrales es ***normalizar el intercambio de asientos registrales entre distintas oficinas de registro (físicas y electrónicas) de documentos de entrada y salida.*** Para ello, establece las condiciones y características del modelo SICRES, la información mínima necesaria para realizar el intercambio de un asiento registral, así como la estructura de dicha información y los requisitos tecnológicos mínimos que deben cumplirse durante el intercambio.

Índice

I - SICRES: Sistema de Información Común de Registros de Entrada y Salida.
II - Objetivo y alcance de esta Norma Técnica de Interoperabilidad
III - Ámbito de aplicación y destinatarios
IV - Modelo de datos para el intercambio de asientos entre Entidades Registrales
IV.1 – Definición y características generales de SICRES 3.0
IV.2 - Estructura y contenido del mensaje de datos de intercambio
IV.3 - Estructura y contenido del mensaje de control
V – Descripción y estados del intercambio
V.1 - Generación del Identificador de Intercambio
V.2 - Estados en el mensaje de datos de intercambio
V.3 - Estados en los mensajes de control
VI - Funciones y requisitos del sistema de intercambio
VI.1 - Requisitos de seguridad
VI.2 - Gestión del proceso de intercambio
VI.3 - Soporte del modo de prueba
VI.4 - Directorio Común
VI.5 - Control y gestión de errores
VI.6 - Comunicación entre distintos sistemas de intercambio
VI.7 - Otras recomendaciones
ANEXO 1: CODIFICACIÓN
ANEXO 2: ESQUEMA XML DEL MODELO DE DATOS SICRES 3.0

NORMAS TÉCNICAS DE INTEROPERABILIDAD EN ELABORACIÓN

Catálogo de estándares: establecerá un conjunto de estándares que satisfagan lo previsto en el artículo 11 del ENI de forma estructurada y con indicación de los criterios de selección y ciclo de vida aplicados.

Protocolos de intermediación de datos: tratará las especificaciones de los protocolos de intermediación de datos que faciliten la integración y reutilización de servicios en las Administraciones públicas y que serán de aplicación para los prestadores y consumidores de tales servicios.

Relación de modelos de datos que tengan el carácter de comunes en la Administración y aquellos que se refieran a materias sujetas a intercambio de información con los ciudadanos y otras administraciones.

Reutilización de recursos de información: tratará de las normas comunes sobre la localización, descripción e identificación unívoca de los recursos de información puestos a disposición del público por medios electrónicos para su reutilización.

GUÍAS CCN-STIC-ENS

El adecuado desarrollo e implantación de lo contenido en la ***Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos***, requiere la formulación de los principios de seguridad tecnológica en el acceso a tales servicios, así como la determinación de las medidas de seguridad que habrán de implantarse por todas las Administraciones Públicas españolas para el normal desenvolvimiento del procedimiento administrativo, en los términos descritos por la ley.

Es precisamente el ***Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica***, en cumplimiento de los dispuesto la precitada norma, el que viene a fijar los ***principios básicos y requisitos mínimos***, así como las **medidas de protección** a implantar en los sistemas de la Administración, y promueve la elaboración y difusión de ***guías de seguridad de las tecnologías de la información y las comunicaciones por parte de CCN (Guías CCN-STIC-ENS, serie 800)*** para facilitar un mejor cumplimiento de dichos requisitos mínimos.

Seguidamente, se hace un breve resumen del contenido de las Guías CCN-STIC-ENS que, a fecha de redacción de este documento, han sido publicadas.

Guía 800:

Glosario de Términos y Abreviaturas del ENS.

Versión disponible: 31 de marzo de 2011 (Borrador)

https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/800-Glosario_de_terminos_y_abreviaturas/800-Glosario_de_terminos_ENS-2011-03-31.pdf

Recoge aquellos ***términos y abreviaturas*** utilizados en las guías de desarrollo del ENS.

*Guía **801**:*

Responsables y Funciones en el Esquema Nacional de Seguridad.

Versión disponible: febrero de 2011

https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/801-Responsabilidades_en_el_ENS/801_ENS-responsabilidades_feb-11.pdf

El mantenimiento y gestión de la seguridad de los Sistemas de Información va íntimamente ligada al establecimiento de una ***Organización de Seguridad***.

Dicha Organización se establece mediante la identificación y definición de las diferentes ***actividades y responsabilidades en materia de gestión de la seguridad*** de los sistemas de información y la implantación de una estructura que las soporte. En consonancia con el artículo 10 del Esquema Nacional de Seguridad:

• En los sistemas de información se diferenciará el responsable de la información, el responsable del servicio y el responsable de la seguridad.

• El responsable de la información determinará los requisitos de la información tratada; el responsable del servicio determinará los requisitos de los servicios prestados; y el responsable de seguridad determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

• La responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la prestación de los servicios.

• La política de seguridad de la organización detallará las atribuciones de cada responsable y los mecanismos de coordinación y resolución de conflictos.

• En esta guía, cuando se habla de "Seguridad", se refiere a "Seguridad de la Información", salvo que se indique algún ámbito específico.

• En esta guía, cuando se habla de "Responsable de la Seguridad", se refiere a "Responsable de la Seguridad de la Información", salvo que se indique explícitamente algún ámbito específico.

El objeto de esta guía es ***crear un marco de referencia que establezca las responsabilidades generales en la gestión de la seguridad*** de los sistemas de información, así como proponer unas figuras o roles de seguridad que asuman dichas responsabilidades.
Es responsabilidad de cada Organismo establecer su propia Organización de Seguridad de acuerdo con sus necesidades y limitaciones.

*Guía **802**:* ***Auditoría del Esquema Nacional de Seguridad.***

Versión disponible: 1 de junio de 2010

https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/802-Auditoria_ENS/802-Auditoria_ENS-jun10.pdf

Esta guía tiene el objetivo de ***encauzar de una forma homogénea la realización de las auditorías, ordinarias o extraordinarias***, estableciendo unas premisas mínimas en su ejecución, sin que por lo tanto, ello implique una limitación en la aplicación de metodologías o esquemas de trabajo propios del equipo de auditoría y la correspondiente emisión de una opinión objetiva e independiente en el informe de auditoría, siempre que se desarrolle dentro de los objetivos y alcances requeridos por el artículo 34.

Esta auditoría es requerida, de forma ordinaria, cada dos años para los sistemas de categoría media y alta, según el Anexo I del RD 3/2010, y con carácter extraordinario, siempre que se produzcan modificaciones sustanciales en el sistema de información, que puedan repercutir en las medidas de seguridad requeridas. La realización de la auditoría extraordinaria determinará la fecha de cómputo para el cálculo de los dos años, establecidos para la realización de la siguiente auditoría regular ordinaria.

La trascendencia e importancia de los resultados de esta auditoría quedan reflejadas en el artículo 34, donde se establece que "En el caso de los sistemas de categoría ALTA, visto el dictamen de auditoría, el responsable del sistema podrá acordar la retirada de operación de alguna información, de algún servicio o del sistema en su totalidad, durante el tiempo que

estime prudente y hasta la satisfacción de las modificaciones prescritas".

El RD 3/2010 establece una serie de requisitos mínimos de medidas de seguridad pero, es posible, que también sean aplicables otros requisitos legales que el auditor debe tener en cuenta (en la medida que no impliquen un nivel inferior de seguridad requerido por este RD 3/2010), o bien que prescriben la realización de auditorías de las medidas de seguridad pero con objetivos o bien alcances diferentes.

Estos requisitos de auditoría adicionales no están dentro del objeto y alcance de la auditoría requerida por el RD 3/2010. Sin embargo, en determinadas situaciones, la necesidad de una mayor eficiencia en la aplicación de los recursos (tanto de auditores como del personal involucrado en el sistema de información auditado) puede aconsejar la realización conjunta de estas auditorías. Aún en estos casos se deben aplicar las premisas mínimas de esta guía para la realización de estas auditorías.

*Guía **803**:*
Valoración de sistemas en el Esquema Nacional de Seguridad.

Versión disponible: 31 de enero de 2011

https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/803-Valoracion_en_el_ENS/803_ENS-valoracion_ene-11.pdf

El proceso de determinación de niveles y categorías se establece en el Anexo I, que aporta una serie de ***criterios generales para determinar si los requisitos de seguridad son de nivel ALTO, MEDIO o BAJO*** en cada una de las dimensiones de seguridad: ***disponibilidad [D], autenticidad [A], integridad [I], confidencialidad [C] y trazabilidad [T].***

El Esquema Nacional de Seguridad establece tres categorías: BÁSICA, MEDIA y ALTA.

• Un sistema de información será de categoría ALTA si alguna de sus dimensiones de seguridad alcanza el nivel ALTO.

• Un sistema de información será de categoría MEDIA si alguna de sus dimensiones de seguridad alcanza el nivel MEDIO, y ninguna alcanza un nivel superior.

• Un sistema de información será de categoría BÁSICA si alguna de sus dimensiones de seguridad alcanza el nivel BAJO, y ninguna alcanza un nivel superior.

En esta guía se busca ***ampliar los criterios para determinar el nivel de seguridad requerido en cada dimensión***. Para ello se analizan los elementos esenciales: información y servicios, pivotando alrededor de ellos los criterios que el responsable de cada información y cada servicio podrá utilizar.

*Guía **804**:*
Medidas de implantación del Esquema Nacional de Seguridad.

Versión disponible: 26 de octubre de 2011 (Borrador)

https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/804-Medidas_de_implantacion_del_ENS/804-Medidas_de_implantacion_del_ENS-20111026.pdf

El Esquema Nacional de Seguridad establece una serie de ***medidas de seguridad en su Anexo II que están condicionadas a la***

valoración del nivel de seguridad en cada dimensión, y a la categoría (artículo 43) del sistema de información de que se trate. A su vez, la categoría del sistema se calcula en función del nivel de seguridad en cada dimensión.

Estas medidas constituyen un mínimo que se debe implementar, o justificar los motivos por los cuales no se implementan o se sustituyen por otras medidas de seguridad que alcancen los mismos efectos protectores sobre la información y los servicios.

Esta guía busca ayudar a los responsables de los sistemas para que puedan implantar rápida y efectivamente las medidas requeridas, sin perjuicio de que empleen recursos propios o recurran a proveedores y productos externos.

Para cada medida se proporciona:

• una descripción más amplia que la proporcionada en el ENS,

• referencias externas que ayuden a su comprensión y realización,

• relación con medidas o controles en otros esquemas de seguridad,

• relación con los principios básicos recogidos en el ENS,

• relación con los requisitos mínimos recogidos en el ENS e

• indicaciones de lo que se considerará evidencia suficiente de cara a una evaluación de la seguridad

*Guía **805**:* ***Política de Seguridad de la Información.***

Versión disponible: septiembre de 2011

https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/805-Politica_de_seguridad_del_ENS/805-ENS_politica-sep11.pdf

La Política de Seguridad de la Información es un documento de alto nivel que define lo que significa 'seguridad de la información' en una organización. El documento debe estar accesible por todos los miembros de la organización y redactado de forma sencilla, precisa y comprensible. Conviene que sea breve, dejando los detalles técnicos para otros documentos normativos.

El Esquema Nacional de Seguridad (ENS) se refiere en varios puntos a la Política de Seguridad:

Artículo 11. Requisitos mínimos de seguridad:
1. Todos los órganos superiores de las Administraciones públicas deberán disponer formalmente de su política de seguridad, que será aprobada por el titular del órgano superior correspondiente.

Artículo 12. Organización e implantación del proceso de seguridad
La seguridad deberá comprometer a todos los miembros de la organización. La política de seguridad según se detalla en el Anexo II, sección 3.1, deberá identificar unos claros responsables de velar por su cumplimiento y ser conocida por todos los miembros de la organización administrativa.
Disposición transitoria. Adecuación de sistemas.
3. Mientras no se haya aprobado una política de seguridad por el órgano superior competente serán de aplicación las políticas de

seguridad que puedan existir a nivel de órgano directivo.
Anexo II Medidas de Seguridad
Marco organizativo [org]
Política de seguridad [org.1]
La política de seguridad será aprobada por el órgano superior competente que corresponda, de acuerdo con lo establecido en el Artículo 11, y se plasmará en un documento escrito, en el que, de forma clara, se precise, al menos, lo siguiente:
a) Los objetivos o misión de la organización.
b) El marco legal y regulatorio en el que se desarrollarán las actividades.
c) Los roles o funciones de seguridad, definiendo para cada uno, los deberes y responsabilidades del cargo, así como el procedimiento para su designación y renovación.
d) La estructura del comité o los comités para la gestión y coordinación de la seguridad, detallando su ámbito de responsabilidad, los miembros y la relación con otros elementos de la organización.
e) Las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.
La política de seguridad debe referenciar y ser coherente con lo establecido en el Documento de Seguridad que exige el Real Decreto 1720/2007, en lo que corresponda.

Esta guía ***propone un modelo genérico de Política de Seguridad de la Información***. El contenido se lista en la sección 3. La sección 4 da pautas para desarrollar dicho contenido. Y el Anexo C muestra un ejemplo que se puede tomar como base para particularizarlo a casos concretos.

*Guía **806**:*
Plan de Adecuación del Esquema Nacional de Seguridad.

Versión disponible: enero de 2011

https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/806-Plan_adecuacion_ENS/806_ENS-adecuacion_ene-11.pdf

El Esquema Nacional de Seguridad, en su Disposición Transitoria sobre Adecuación de los Sistema, dice que:

1. Los sistemas existentes a la entrada en vigor del presente real decreto ***se adecuarán al Esquema Nacional de Seguridad*** de forma que permitan el cumplimiento de lo establecido en la disposición final tercera de la Ley 11/2007, de 22 de junio. Los nuevos sistemas aplicarán lo establecido en el presente real decreto desde su concepción.

2. Si a los doce meses de la entrada en vigor del Esquema Nacional de Seguridad hubiera circunstancias que impidan la plena aplicación de lo exigido en el mismo, se dispondrá de un ***Plan de Adecuación*** que marque los plazos de ejecución los cuales, en ningún caso, serán superiores a 48 meses desde la entrada en vigor.

El plan indicado en el párrafo anterior será elaborado con la antelación suficiente y aprobado por los órganos superiores competentes.

Esta guía propone un modelo genérico de Plan de Adecuación.

*Guía **807**:*
Criptología de empleo en el Esquema Nacional de Seguridad.

Versión disponible: septiembre de 2011

https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/807/807-Criptologia_de_empleo_ENS-sep11.pdf

El desarrollo de la sociedad actual repercute en la administración del estado al tener que actualizar ésta los sistemas electrónicos con el fin de proporcionar a los ciudadanos los mismos servicios electrónicos que ofrece de forma local. Tal actualización supone una ***remodelación la seguridad de los sistemas para su adaptación a los nuevos requisitos y posibles amenazas***.

El ***Centro Criptológico Nacional (CCN)*** lleva años trabajando en la securización, evaluación y acreditación de los sistemas de información de la administración del estado, además de la formación del personal de dicha administración.

Dentro de la estructura del CCN se encuentra el ***Organismo de Certificación (OC)*** del Centro Criptológico Nacional que comprende a las entidades públicas o privadas que deseen ejercer como laboratorios de evaluación de la seguridad de las Tecnologías de la Información (TI) en el marco del Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información (ENECSTI). También incluye a las entidades públicas o privadas que sean fabricantes de productos o sistemas de TI que pretendan certificar la seguridad de sus productos en el marco del ENECSTI (véase http://www.oc.ccn.cni.es/index_es.html para mayor información). Los certificados "Common Criteria" emitidos por el Organismo de Certificación están reconocidos internacionalmente por más de veinte países. Además, el OC está acreditado por la Entidad Nacional de Acreditación, conforme a los criterios recogidos en la Norma UNEEN 45011:1998 para la certificación de productos.

Por esta razón los sistemas, productos y equipos evaluados y certificados por el CCN cumplen los requisitos de funcionalidad que tales productos afirman verificar en la declaración de seguridad.

Guía 808:
Verificación del cumplimiento de las medidas en el Esquema Nacional de Seguridad.

Versión disponible: septiembre de 2011 (Borrador)

https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/808/808-Verificacion_del_cumplimiento_medidas_ENS-sep11.pdf

El Esquema Nacional de Seguridad (Real Decreto 3/2010 de 8 de enero), en su artículo 34 (Auditoría de la seguridad) y en su Anexo III (Auditoría de la seguridad), establece la obligatoriedad de la realización de una auditoría de seguridad para los sistemas de categoría media y alta de forma ordinaria cada dos años, o de forma extraordinaria cada vez que se produzcan modificaciones sustanciales en el sistema de información.

La presente guía viene a complementar a la guía "CCN-STIC-802 Esquema Nacional de Seguridad – Guía de auditoría".

El objeto de esta guía es que sirva tanto de itinerario, como de registro, a aquella persona designada como auditor de los requisitos del Esquema Nacional de Seguridad para un sistema.

Esta guía es de ***aplicación a cualquier entidad pública española que deba cumplir con los preceptos de la Ley de Acceso Electrónico de los Ciudadanos a los Servicios Públicos*** (Ley 11/2007 de 22 de junio), de la que emana el Esquema Nacional de Seguridad (Real Decreto 3/2010 de 8 de enero), con independencia de su naturaleza o dimensión y cuyos sistemas se hayan clasificado como de nivel medio o alto.

*Guía **809**:*
Declaración de Conformidad del Esquema Nacional de Seguridad.

Versión disponible: 29 de julio de 2010 (Borrador)

https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/809-Declaracion_de_conformidad_ENS/809-Declaracion_de_conformidad_ENS_2010-07-29.pdf

La presente Guía tiene por objeto ***dar pautas generales para la aplicación de lo dispuesto en el artículo 41 del Esquema Nacional de Seguridad***, sin perjuicio de la particularización de cada organismo.

El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica dedica su capítulo VIII a las normas de conformidad. El artículo 41 preceptúa que los órganos y entidades de derecho público ***darán publicidad en las correspondientes sedes electrónicas a las declaraciones de conformidad, y a los distintivos de seguridad de los que sean acreedores***, obtenidos respecto al cumplimiento del Esquema Nacional de Seguridad.

*Guía **810**:*
Creación de un CERT / CSIRT.

Versión disponible: 15 de septiembre de 2011 (Borrador)

https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/810-Creacion_de_un_CERT-CSIRT/810-Guia_Creacion_CERT-CSIRT.pdf

El uso masivo de las tecnologías de la información en todos los ámbitos de la sociedad, así como ***la convergencia e interconexión de los sistemas ha venido generando nuevos riesgos y vulnerabilidades*** en todas las organizaciones que se ven presionadas diariamente por el creciente número de amenazas que ponen en peligro sus activos, en algunos casos, realmente críticos para su funcionamiento. Estas amenazas en el ciberespacio, que en gran medida siguen siendo las mismas que en el mundo físico (fraude, robo, espionaje industrial, terrorismo, sabotaje…) se han visto agravados por la rentabilidad de los ataques automatizados, la acción a distancia y las técnicas de propagación cada día más rápidas y fáciles de emplear. De igual modo, los ataques han ido ganando en complejidad, sigilo y focalización y especialización en los objetivos, siendo, por tanto, más compleja su resolución (la dificultad en hacer frente a amenazas como rookits, troyanos, ataques dirigidos, denegaciones de servicio distribuidas – DDoS – o las botnets, es mucho mayor que las amenazas evidentes como el spam, phishing, virus, gusanos, adware, etc.).

El panorama descrito obliga a las organizaciones, bien sean públicas o privadas, a realizar un ***esfuerzo adicional en preservar la seguridad de sus sistemas y responder a estos nuevos riesgos e incidentes***. Una preservación que requiere de una política de seguridad integral y, especialmente, del desarrollo de unos servicios y capacidades operativas específicas en materia de operación y respuesta ante incidentes de seguridad.

De este modo, en los últimos años, se han venido desarrollando ***estructuras orientadas a la operación y gestión de incidentes de seguridad, llamados CERT (Computer Emergency Response Team) o CSIRT (Computer Security Incidente Response Team)***, como solución más adecuada para dar una respuesta eficaz y eficiente a estos nuevos riesgos.

*Guía **811**:*
Interconexión en el Esquema Nacional de Seguridad.

Versión disponible: 14 de septiembre de 2011 (Borrador)

https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/811-Interconexion_en_el_Esquema_Nacional_de_Seguridad/811-Interconexion_en_el_ENS.pdf

En los últimos años hemos asistido a un desarrollo sin precedentes en la sociedad de la información, ***la generalización de las conexiones de banda ancha*** y la cada vez mayor alfabetización digital han contribuido a un nuevo escenario donde el ciudadano demanda facilidad y flexibilidad de acceso a los servicios prestados por la administración pública.

Leyes como la 11/2007 reconocen el derecho de los ciudadanos a relacionarse con las administraciones públicas electrónicamente y la obligación de las mismas de garantizar este derecho, planteando a su vez un importante desafío a nivel tecnológico para los diferentes organismos, que han visto aumentar la complejidad de sus sistemas a la par que las interrelaciones y conexiones con otras entidades.

La finalidad del Esquema Nacional de Seguridad es la creación de las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos, que permita a los ciudadanos y a las Administraciones públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios. La manera y forma en que los sistemas de los diferentes organismos públicos se interconectan debe adecuarse a este nuevo marco de trabajo y es en esta función en la que esperamos esta guía sirva de ayuda.

El Esquema Nacional de Seguridad (Real Decreto 3/2010 de 8 de enero), en su artículo 22 ("Prevención ante otros sistemas de información interconectados"), establece la ***obligatoriedad de proteger el perímetro de los sistemas a interconectar, (en particular si se utilizan redes públicas total o parcialmente) y de analizar los riesgos derivados de la interconexión de los sistemas, controlando además su punto de unión.***

Esta guía pretende ***ayudar en la toma de decisiones a las personas involucradas en la interconexión de sistemas*** cubiertos por el Esquema Nacional de Seguridad.

*Guía **812**:*
Seguridad en Entornos y Aplicaciones Web.

Versión disponible: 26 de octubre de 2011 (Borrador)

https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/812-Seguridad_en_Entornos_y_Aplicaciones_Web/812_Entornos-y-aplicaciones-web_20111026.pdf

Dada la ***criticidad tanto de los entornos de producción*** como de los dispositivos embebidos, se hace necesario establecer una metodología que permita evaluar y reforzar la seguridad de los entornos y aplicaciones Web asociados a éstos.

Desde el punto de vista de la seguridad, todos los elementos que conforman el entorno o aplicación Web descritos en el punto previo deben ser tenidos en cuenta a la hora de evaluar y diseñar los mecanismos de protección.

El presente documento establece unas

pautas de carácter general enfocadas a las características propias de las aplicaciones y servicios web para establecer una política de seguridad en dichos sistemas teniendo en cuenta los requerimientos establecidos en el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. Se espera que cada organización las particularice para adaptarlas a su entorno singular.

*Guía **814**:*
Seguridad en correo electrónico.

Versión disponible: 31 de agosto de 2011 (Borrador)

https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/814-Seguridad_en_Correo_Electronico/814_Seguridad-en-correo-electronico.pdf

El correo electrónico es hoy en día uno de los mecanismos de intercambio de información más utilizados, tanto en el ámbito personal como en el profesional. Todas las personas que utilizan Internet en su trabajo o en su hogar disponen de una o más cuentas de correo electrónico, cuentas que, como veremos más adelante, sufren a diario ataques de todo tipo con el objetivo principal de robar información.

El envío de correo electrónico es, desde el punto de vista del usuario, un proceso completamente transparente: escribimos un mensaje, rellenando unos campos concretos (como el receptor o el asunto) y lo enviamos desde un cliente concreto, apareciendo al poco tiempo el mensaje en el buzón de su destinatario. No obstante, este proceso, como hemos dicho transparente para el usuario, lleva asociados una serie de elementos tecnológicos y de protocolos de transporte y acceso que es necesario conocer para poder hablar de la seguridad en el correo electrónico.

Desde un punto de vista técnico y de seguridad, podemos diferenciar dos partes en un correo electrónico: el cuerpo y las cabeceras. La primera está formado por el contenido del mensaje en sí (incluyendo posibles adjuntos, previamente tratados para poderse transmitir), y por tanto depende por completo de lo que el usuario haya decidido incluir en dicho mensaje. La segunda parte a la que hacíamos referencia, las cabeceras, contiene información tanto facilitada de una u otra forma por el usuario (asunto, destinatario, emisor…) como añadida por el servidor o servidores por los que pasa el mensaje hasta llegar a su destino.

Estas cabeceras son importantes para determinar algunos aspectos de seguridad de los correos electrónicos; en especial para conocer el camino que un mensaje ha seguido entre emisor y receptor, ya que cada vez que el mensaje pasa por un servidor de correo éste añade un campo de datos a las cabeceras, con etiqueta Received, especificándose el nombre del servidor, su dirección IP, el servidor de correo utilizado, y la fecha y la hora en que se recibió el mensaje. De esta forma podemos determinar si un correo proveniente de un cierto dominio de Internet se ha procesado efectivamente en servidores relacionados con dicho dominio o por el contrario viene de sistemas que a priori no son propios del mismo, lo que indicaría que el mensaje puede haber sido falseado.

*Guía **815**:*
Métricas e Indicadores en el Esquema Nacional de Seguridad.

Versión disponible: 10 de diciembre de 2011 (Borrador)

https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/815-Metricas_e_Indicadores_en_el_ENS/815_metricas_e_indicadores_ENS.pdf

El Esquema Nacional de Seguridad (ENS) establece la obligación de evaluar regularmente el estado de seguridad de los sistemas:

Artículo 35. Informe del estado de la seguridad. El Comité Sectorial de Administración Electrónica articulará los procedimientos necesarios para conocer regularmente el estado de las principales variables de la seguridad en los sistemas de información a los que se refiere el presente real decreto, de forma que permita elaborar un perfil general del estado de la seguridad en las Administraciones públicas.

Así mismo, el ENS ***establece la necesidad de establecer un sistema de medición de la seguridad del sistema en el Anexo II*** – Medidas de seguridad.

Esta guía busca una ***sistematización de ambas obligaciones por medio de la definición de un conjunto ordenado de indicadores que puedan ser utilizados en diferentes momentos y circunstancias*** según convenga, pero con una definición uniforme.

Documentación preparada por:

Carlos Galán *es Doctor en Informática, Abogado especialista en Derecho de las Tecnologías de la Información, Certified Information Security Manager (CISM) por ISACA, Consultor/Formador Homologado de la EOI, Presidente de la Agencia de Tecnología Legal y Profesor de la Universidad Carlos III de Madrid.*

www.clubdeinnovacion.es

Club de Innovación

Colaboramos con las administraciones

Fomentamos la innovación

Más información:

Web: http://www.clubdeinnovacion.es

Facebook: facebook.com/CLUBDEINNOVACION

Twitter: @clubdeinnovacio

Linkedin: http://es.linkedin.com/in/clubdeinnovacion

"Al servicio de las Administraciones Públicas y las empresas innovadoras "
Club de Innovación tiene como misión difundir y fomentar la innovación en el ámbito de las Administraciones Públicas.

Para ello ofrece:

Información. A través de su portal de buenas prácticas de innovación y modernización para poner al alcance de los responsables públicos las experiencias de otras administraciones y las propuestas de las empresas más innovadoras.

Formación y debate. A través de su oferta de cursos, jornadas y congresos de innovación destinados a las administraciones.

El portal presenta de forma gratuita más de 500 buenas prácticas para su consulta y ofrece información actualizada sobre noticias, normativas, informes, publicaciones, agenda de eventos, blogosfera y novedades, siempre relacionados con la innovación y la modernización de la administración, de interés para los responsables públicos.

Las actividades de formación y debate se realizan bajo el criterio de estrecha colaboración "con y para las administraciones públicas", presentando ofertas de interés para éstas y para los empleados públicos a los que se dirige.

Club de Innovación es especialmente activo en la difusión y el fomento de la aplicación de los Esquemas Nacionales de Interoperabilidad y Seguridad habiendo "coorganizado" con diferentes comunidades, diputaciones y ayuntamientos una decena de jornadas de formación sobre la "Introducción y aplicación de los EE.NN. en las AA.PP."

El II Congreso CNIS 2012 es la reafirmación de la "innovadora fórmula de colaboración público-privada" que aporta Club de Innovación a nuestras empresas y administraciones.

Patrocinador Platino

Telefónica

Telefónica Grandes Empresas. Sector AA.PP

Conectamos con la Administración Pública. Nuevos tiempos, nuevas soluciones

La Administración Pública evoluciona al ritmo de las demandas de la sociedad del conocimiento. Un entorno que cambia a gran velocidad con una nueva generación de ciudadanos participativos que "piensan en red" y se relacionan cada vez más de forma virtual.

Consciente de su papel protagonista como usuaria e impulsora de las TIC, debe asumir y liderar los restos asociados a la implantación de las nuevas tecnologías para impulsar una Sociedad del Conocimiento para todos, lograr una mayor identificación y acercamiento al ciudadano, mejorar las herramientas y la motivación del empleado público, actuando siempre con criterios de productividad, colaboración y eficiencia.

En Telefónica compartimos esa misma visión y también estamos comprometidos con el futuro. Por eso queremos ayudarle facilitando soluciones tecnológicas que, inteligentemente aplicadas, contribuyan a dar respuesta a sus retos.

Más información:

Web: http://www.grandesclientes.telefonica.es/

Twitter @TelefonicaGGCC

Patrocinadores Oro

GTT

Gestión Tributaria Territorrial

Somos una empresa líder en colaborar con las Administraciones Tributarias Locales en la prestación de servicios de primer nivel.

Prestamos servicios profesionales que cubren todo el espectro de posibles necesidades, desde la identificación de escenarios de mejora de los ingresos hasta la colaboración en la gestión.

Contamos con un Sistema de Información que es reconocido en el sector como el de mayor alcance funcional y más avanzado tecnológicamente, que en la actualidad es el soporte para la gestión tributaria y la recaudación de más de 2700 Ayuntamientos a nivel nacional.

Nuestro Sistema tiene integrados todos los mecanismos de interoperabilidad "on-line" existentes, con las Instituciones que ofrecen este tipo de servicios en la actualidad, en cuyo desarrollo y evolución participamos activamente.

Prestamos servicios tecnológicos integrales, bajo el modelo de "cloud computing", reduciendo de este modo la inversión necesaria y acortando los plazos de puesta en marcha.

Buscamos permanentemente mejorar la eficiencia tributaria. Todos nuestros clientes han incrementado sus ingresos tributarios y han mejorado la calidad del servicio que prestan a sus ciudadanos.

Implantamos la Administración Electrónica Integral en la gestión de ingresos, desde la gestión de expedientes sin papeles a la tramitación on-line con validez jurídica.

Más información:

Avda. Miriam Blasco, 1-bis
03016 Alicante

Telf. 965268384

gtt@gtt.es
www.gtt.es

Ges consultor

El cumplimiento del E.N.S y otra normativa relacionada como el E.N.I. o el Plan Nacional de Infraestructuras Críticas plantean nuevos retos a las Administraciones en cuanto a la Gestión y Gobierno de sus T.I., de sus Riesgos y del Cumplimiento con las nuevas obligaciones y marcos regulatorios. GESCONSULTOR le proporciona una solución integral:

PLATAFORMA G.R.C.:
CUADROS DE MANDO
AUTOMATIZACIÓN DE PROCESOS
SINGLE SIGN ON

GESTIÓN DEL CUMPLIMIENTO:
· ENS
· ENI
· PRIVACIDAD
· ISO 27001
· PCI-DSS
· INTEGRACIÓN CON GESDATOS
· CONTINUIDAD (PNIC)
· ISO 9001
· ITIL / ISO 20000

GESTIÓN DEL RIESGO:
· MOTOR DE RIESGOS ISO
· SOPORTE COMPLETO MAGERIT
· INTEGRACIÓN CON P.I.L.A.R.

SOLUCIONES OPERATIVAS Y DE ADMINISTRACIÓN
· INTEGRACIÓN CON SU INFRAESTRUCTURA
· SOLUCIONES OPEN-SOURCE INTEGRADAS
· CMDB
· SERVICE DESK
· MONITORIZACIÓN
· GESTIÓN DOCUMENTAL
· E-LEARNING
· SIEM – MONITORIZACIÓN DE EVENTOS DE SEGURIDAD Y RIESGOS EN TIEMPO REAL

Más información:

VALENCIA: Avda. Cortes Valencianas, 50, 1 C 46015 - Valencia
MADRID: Paseo de la Castellana, 153 28046 – Madrid

Teléfono de contacto: 902 900 231
Email: info@gesconsultor.com
Web: www.gesconsultor.com

Tecnocom

Multinacional española, que cotiza en la Bolsa de Madrid desde 1987. Cuenta con cerca de 6.000 empleados, operando en España, Portugal y América Latina.
Con presencia en todos los sectores, estructurados de la siguiente manera: Financiero y Seguros, Administraciones Públicas, Telco y Media e Industria.

Posee amplia experiencia en el sector público, desarrollando numerosos proyectos de administración electrónica, interoperabilidad, gestión de tributos, interconexión de juzgados, tarjeta ciudadana, sanidad y educación.

La diferenciación de la propuesta de valor de Tecnocom se basa en ofrecer soluciones a medida a sus clientes, gracias al extenso conocimiento de sus procesos de negocio.

Tecnocom apuesta por una Administración Pública interoperable y ha diseñado una solución para permitir a los organismos públicos lucir su declaración de conformidad con el Esquema Nacional de Interoperabilidad de la mejor manera posible, sin gastos excesivos y con la mayor calidad.

Más información:

C/ Josefa Valcárcel, 26
28027 Madrid

Telf. 901 900 900

info@tecnocom.es
www.tecnocom.es

BlackBerry

Fundada en 1984, Research In Motion (RIM), líder mundial en innovación inalámbrica, revolucionó la industria de los móviles con el lanzamiento de la solución BlackBerry en 1999. Hoy en día, 75 millones de clientes en todo el mundo utilizan los productos y servicios de BlackBerry para mantenerse en contacto con las personas y el contenido que más les importa en su día a día.

La solución BlackBerry se ha diseñado para asegurar que todas las comunicaciones se realizan en una infraestructura segura. RIM continúa trabajando para crear productos innovadores pero siempre preservando la seguridad y eficiencia de una solución robusta que cumple con las necesidades de sus clientes corporativos, institucionales o particulares.

Con 50 millones de usuarios, RIM posee además una plataforma social líder, BlackBerry Messenger (BBM).
A través de las herramientas que Research In Motion ofrece a los desarrolladores, los usuarios tienen a su alcande más de 60.000 aplicaciones, que han alcanzado las 2.000 millones de descargas en 2012.
RIM cotiza en el NASDAQ (NASDAQ: RIMM) y en la Bolsa de Toronto (TSX: RIM).

Más información:

C/ Caleruega 102-104
28033 Madrid

Twitter. @blackberryESP
www.blackberry.es

Vortal

La plataforma electrónica de contratación para el sector público de Vortal, vortalGOV, integra y simplifica los procesos de adjudicación entre Administraciones Públicas y empresas privadas, ya que es capaz de gestionar de manera electrónica y sin papeles todos los pasos –desde la publicación de los pliegos hasta la adjudicación- en una sola estructura de una forma rápida, transparente, segura y con la máxima confidencialidad.

El principal beneficio que ofrece esta plataforma de contratación para Administraciones Públicas y licitadores es el ahorro de hasta un 30% de los costes de gestión y adjudicación de los procedimientos.

vortalGOV es una solución "Cloud Computing" versátil y fácil de integrar con el resto de sistemas de gestión existentes en las distintas Administraciones Públicas y, al no estar ligada a un dispositivo tecnológico específico proporciona mayor flexibilidad a los usuarios, ya que pueden acceder a la plataforma en cualquier momento y desde cualquier lugar como, por ejemplo, teléfonos móviles.

Más información:

Calle Jazmín 66
28033 Madrid

Telf. 91 302 94 00

jose.aristegui@vortal.es
www.vortal.es y www.vortalgov.es

Indra

Indra colabora con las Administraciones Públicas creando soluciones y servicios de valor para el ciudadano, consiguiendo un mayor acercamiento y promoviendo la participación de la ciudadanía en las iniciativas públicas, haciendo que la Administración sea más accesible y facilitando el trabajo diario de los empleados públicos.

Indra cuenta con experiencia y personal experto en la problemática específica de la Administración, lo cual ha permitido un mejor entendimiento con sus clientes y una rápida y efectiva aportación de soluciones y servicios. Gracias a esto, la oferta de soluciones y servicios de Indra tiene un éxito contrastado, no sólo entre las propias entidades públicas, sino también, y quizás más importante, entre los ciudadanos.

Una oferta especializada para competir con éxito en los mercados internacionales durante los últimos años, Indra ha apostado por una especialización de su oferta para las administraciones públicas, mediante la incorporación a sus soluciones y servicios de funcionalidades dirigidas específicamente a resolver las necesidades concretas en administración electrónica.

2/3 de las Comunidades Autónomas españolas cuentan con soluciones de administración electrónica de Indra.

Más información:

Avenida de Bruselas, 35
28108 Alcobendas

Telf. 91 480 68 14

gsanchezvizcaino@indra.es
www.indracompany.com/

Santander

Banco Santander
Banca Institucional

En Banco Santander contamos con un área especializada en Instituciones, Santander Banca Institucional, que ofrece a las Instituciones Públicas el tratamiento especializado, exclusivo e innovador que éstas demandan de las entidades financieras.

Sabemos que las Instituciones requieren una oferta de productos y servicios adaptados a sus necesidades. Para ello, Santander Banca Institucional coordina a las diferentes áreas especializadas en productos y servicios de nuestro Grupo. De esta forma, nuestros clientes institucionales reciben un tratamiento global, profesional y directo bajo la supervisión de un gestor especializado, dando respuestas personalizadas, y por tanto ágiles y eficientes.

Somos conscientes de los retos que la Administración debe asumir en todos los ámbitos y desde Banco Santander mantenemos nuestro compromiso con este sector.

Más información:

Acuda a nuestras oficinas Santander

Telf. 902 24 24 24

bancainstitucional@gruposantander.com
www.bancosantander.es

Colaboran

Ingenia

Ingenia es una compañía de tecnologías de la información, especializada en servicios y soluciones en torno a internet y nuevos medios, y con líneas estratégicas de negocio en comunicaciones, ingeniería y sistemas, formación y gestión del talento, y en desarrollo software.

Con veinte años de experiencia en el sector, cuenta con sedes en Málaga, Sevilla, Madrid, Barcelona y Chile; un centro de trabajo en Ronda, una delegación en México, negocios en Argentina, Jordania, Marruecos.

Más información:

Calle Severo Ochoa, 43
29590 Campanillas (Málaga)

Telf. 952 02 93 00

info@ingenia.es
www.ingenia.es

T-Systems

Con una infraestructura de centros informáticos y redes a nivel mundial, T-Systems ofrece tecnologías de la información y de la comunicación (TIC) a grupos multinacionales e instituciones públicas. Sobre esta base, la filial de servicios para empresas de Deutsche Telekom facilita soluciones integradas para un futuro en red entre las empresas y la sociedad. Unos 47.600 empleados combinan experiencia en cada sector, e innovación TIC para agregar un notable valor añadido al negocio principal de de sus clientes en todo el mundo. T-Systems obtuvo unos ingresos de alrededor de 9.100 millones de euros en el ejercicio 2010.

Más información:

Sancho de Ávila, 110 - 130
08018 Barcelona

Telf. 93 501 50 00

marketing@t-systems.es
www.t-systems.es

Nae

Nae es una consultora global en el ámbito de la sociedad de la información, que trabaja para contribuir al éxito de la estrategia de sus clientes gracias a su conocimiento de la tecnología, organización, procesos y modelos de negocio. Con un equipo de 70 profesionales con una amplia experiencia, Nae aporta soluciones específicas y personalizadas a las necesidades concretas de sus clientes, entre los que se encuentran Operadores de Telecomunicación, Administraciones Públicas y Grandes Corporaciones.

En los últimos años Nae ha colaborado y asesorado a varios de sus clientes ayudándoles en la definición de sus estrategias de adecuación al Esquema Nacional de Seguridad y al Esquema Nacional de Interoperabilidad y en la implantación de los mismos.

Nae cuenta con oficinas en Barcelona, Madrid, Valencia, Zaragoza, Cáceres y Lisboa y una facturación prevista para finales de 2012 superior a los seis millones de Euros.

Más información:

Telf. 913 923 655 / 934 949 960

info@nae.es
www.nae.es

Deloitte

DELOITTE ENTERPRSISE RISK SERVICES (IT ERS) (España) Desde 1989, cuenta con 221 profesionales, ofreciendo sus servicios especializados a las Industrias Financiera, de Telecomunicaciones, Medios, Energía y Productos y Servicios.

Líderes como proveedores de auditoría de calidad de los sistemas de información y proveedores de consultoría técnica relacionada con la gestión, control, seguridad e integridad de los Sistemas de Información.

Promueve políticas de formación continua y obtención y mantenimiento de certificaciones (CISSP, CISA, CISM, SAP, BS 7799/27001, BS 25999, ITIL, CIA, CEH, CRISC, CGEIT).

Sus profesionales son miembros de ISACA, BSI, Instituto de Auditores Internos, Asociación Española de Métricas de Software, Society for Information Management, siendo patrocinadores e instructores de los Másters de Auditoría Informática y Seguridad Informática de la Universidad Politécnica de Madrid. Ponentes habituales en eventos relacionados con seguridad informática. El área de Riesgos Tecnológicos de Deloitte cuenta con laboratorios de Seguridad en Barcelona y Madrid.

Más información:

Plaza de Pablo Ruiz Picasso nº1. Torre Picasso
28020 Madrid

Telf. 914381613

cechegoyen@deloitte.es
www.deloitte.es

Yerbabuena

Yerbabuena Software es una empresa especializada en el desarrollo de Sistemas de Gestión Documental (SGD). Athento es la apuesta bandera de Yerbabuena, una plataforma de Gestión Documental Inteligente que otorga una capa de Interoperabilidad permitiendo la conexión de aplicaciones de terceros con un SGD, facilitando el cumplimiento de las Normas Técnicas de Interoperabilidad. Athento soporta las NTI de documento y expediente electrónico, políticas de firma, copia auténtica, digitalización, etc.

Además, esta plataforma de gestión documental inteligente permite adaptar el Registro de Entrada, el tramitador de flujos, @firma y otras herramientas asociadas a la ley 11/2007 a las normas Técnicas de Interoperabilidad sin incurrir en grandes desarrollos.

Athento se conecta con los principales SGD del mercado como Alfresco, Documentum, Nuxeo, Sharepoint, entre otros, proporcionando a la AAPP la libertad de elegir el que mejor se adapte.

Yerbabuena a día de hoy trabaja con diferentes corporaciones en la adaptación al ENI como son la DGT o la Diputación de Málaga y en empresa privada con corporaciones como BBVA unidad inmobiliaria, EADS en la cadena de producción.

Más información:

C/ Ivan Pavlov 2, Planta 2, Oficina 3, Parque Tecnológico de Andalucía
29590 Málaga-Madrid-Sevilla-San José

Telf. 902 99 52 46

yerbabuena@yerbabuena.es
www.yerbabuenasoftware.com

mimacom

Mimacom es un grupo internacional con sede central en Suiza. Desde sus inicios, mimacom se ha centrado en el desarrollo de software open source y productos J2EE/ Java, "… the open source integrator".

Una de sus iniciativas recientes ha sido participar junto a Experience y Yaco en la creación de una nueva plataforma de administración electrónica interoperable. TangramBPM nace de la alianza de tres empresas con una misma visión: una plataforma de Administración Electrónica completa, ágil, flexible, escalable, de fácil implantación, y a coste muy, muy razonable. Es decir, una Plataforma de AE de nueva generación. Las plataformas nacidas en la primera década del siglo han adolecido de un conjunto de defectos: incompletitud, poca integración, rígidas, poco adaptables a las exigencias de cada Administración, etc. Por el contrario, TangramBPM busca desde su diseño original evitar estos inconvenientes con una arquitectura y una tecnología abiertas, flexibles y basadas en los estándares y productos Open Soiurce más difundidos y actuales: JAVA, Alfresco, Liferay, WSO2, Activiti, etc.

Junto a los módulos nativos de TangramBPM, se pueden integrar componentes y productos que provengan de otro origen si así lo prefiere el usuario. La Plataforma se puede implementar en su totalidad o por módulos, en un solo proyecto o en proyectos sucesivos, y se puede escalar según capacidades requeridas. Una de sus características diferenciales más destacadas es su orientación a Gestión Documental, BPM e Interoperabilidad. Y, sin duda, aspira a colaborar en el pleno éxito de la Ley 11/2007 y de los Esquemas Nacionales de Seguridad e Interoperabilidad.

Más información:

Avda. Cortes Valencianas, 39 – 2º (Edificio Géminis) Center
46015 Valencia

Telf. 961199619

info@mimacomiberica.es
www.mimacom.com

MDtel

MDtel es una compañía especializada en comunicaciones de empresa para mediana y gran empresa.

Desarrollamos todo tipo de proyectos a medida de comunicaciones voz/datos, seguridad e infraestructuras y ofrecemos una extensa gama de soluciones concebidas para que nuestros clientes afronten satisfactoriamente los retos del siglo XXI.

Nuestro portfolio de servicios incluye desde la consultoría e ingeniería de redes hasta el mantenimiento integral de todas sus comunicaciones, pasando por la implementación e instalación de las mismas. Especializada en prestar un servicio postventa de excelencia.

Dispone de recursos técnicos a nivel nacional permitiendo satisfacer unos Niveles de Servicio rigurosos en atención y tiempos e respuesta.

Más información:

C/ Manuel Tovar, 38
28034 Madrid

Telf. 913346100

clientes @mdtel.es
www.mdtel.es

Bilbomática

Bilbomática es una empresa de consultoría e ingeniería de software de capital 100% español, orientada a la generación de soluciones en el ámbito de tecnologías de la información y las comunicaciones.
Bilbomática está especializada en el diseño, desarrollo e implantación de soluciones en los distintos ámbitos de las Administraciones Públicas, siendo nuestros rasgos característicos la calidad, la excelencia en el servicio y la orientación al cliente.

Apostamos por un modelo de Administración Electrónica que integra productos innovadores propios y externos, así como servicios que permitirán a cada Administración incorporar, paso a paso, las piezas necesarias para convertirse en una completa Administración digital.

Para ello, ponemos a disposición de las Administraciones diferentes soluciones tecnológicas cuyo objetivo es optimizar la gestión de las mismas, mejorar la planificación de los servicios, y perfeccionar la ejecución de las prestaciones, desplegando un catálogo de posibilidades que permitan la modernización y el cumplimiento de la cooperación interadministrativa obligatoria e imprescindible para la seguridad y la interoperabilidad entre las distintas administraciones públicas

Más información:

Calle O'Donnell, 34 - 4º Izquierda
28009 Madrid

Telf. 915782790

administracionmadrid@bilbomatica.es
www.bilbomatica.es

Software AG

Software AG es líder mundial en excelencia de procesos de negocio. En nuestros más de 40 años dedicados a la innovación, hemos creado entre otros productos Adabas, la primera base de datos transaccional de alto rendimiento; ARIS, primera plataforma de análisis de procesos de negocio, y webMethods, el primer servidor B2B y plataforma de integración basada en SOA. Software AG tiene una especial penetración en el sector de las Administraciones Públicas.

Somos los únicos del mundo que ofrecemos soluciones completas y sencillas para la gestión de procesos de negocio (BPM), con el coste total de propiedad más bajo. Nuestras marcas líderes en la industria, ARIS, webMethods, Adabas, Natural, Terracotta e IDS Scheer Consulting, representan un porfolio único para: estrategias de procesos, diseño, integración y control; gestión de datos e integración basada en SOA; implementación SAP gestionada por procesos, así como consultoría y servicios estratégicos de procesos.

Software AG ha tenido en 2011 unos ingresos cercanos a los 1.100 millones de euros y cuenta con más de 5.600 empleados que atienden a unos 10.000 clientes de empresas e instituciones públicas distribuidas por 70 países. Nuestras completas soluciones de servicios y software permiten a las compañías alcanzar sus resultados de negocio, más rápido. La sede central de la empresa se encuentra en Alemania y cotiza en la Frankfurt Stock Exchange.

Más información:

Ronda de la Luna, 22
28760 Tres Cantos (Madrid)

Telf. 918079400

marketing@softwareag.es
www.softwareag.es

Notas

ALMERÍA HUESCA LAS PALMAS DE GRAN CANARIA SANTANDER ÁVILA ALBACETE BARCELONA CEUTA MELILLA MADRID PAMPLONA/IRUÑA ALICANTE/ALACANT BADAJOZ A CORUÑA PALMA LOGROÑO BILBAO OVIEDO MURCIA CÁDIZ TERUEL SANTA CRUZ DE TENERIFE BURGOS CIUDAD REAL GIRONA CASTELLÓN DE LA PLANA CÁCERES LUGO DONOSTIA-SAN SEBASTIÁN CÓRDOBA ZARAGOZA LEÓN OVIEDO VALENCIA OURENSE VITORIA-GASTEIZ GRANADA PALENCIA GUADALAJARA TARRAGONA PONTEVEDRA HUELVA SALAMANCA TOLEDO JAÉN SEGOVIA MÁLAGA SORIA SEVILLA VALLADOLID ZAMORA

La Moneda de su Ciudad

TERCERA EMISIÓN

MONEDAS DE COLECCIÓN EN PLATA DE LEY

52 MONEDAS DEDICADAS A LAS CAPITALES DE PROVINCIA Y CIUDADES AUTÓNOMAS

La Real Casa de la Moneda continúa con la serie de **52 Monedas de Colección**, dedicada a las **Capitales de Provincia y Ciudades Autónomas**

Hasta ahora se han emitido 22 monedas: Almería, Huesca, Las Palmas de Gran Canaria, Santander, Ávila, Albacete, Barcelona, Ceuta, Melilla, Madrid, Pamplona/Iruña, Alacant/Alicante, Badajoz, A Coruña, Palma, Logroño, Bilbao, Oviedo, Murcia, Cádiz, Teruel y Santa Cruz de Tenerife (*)

AHORA LES PRESENTAMOS LAS 10 SIGUIENTES

23. BURGOS

24. CIUDAD REAL

25. GIRONA

26. CASTELLÓN DE LA PLANA/ CASTELLÓ DE LA PLANA

27. CÁCERES

28. LUGO

29. DONOSTIA-SAN SEBASTIÁN

30. CÓRDOBA

31. ZARAGOZA

32. LEÓN

P.V.P. (**) 35,40 € CADA MONEDA

CARACTERÍSTICAS TÉCNICAS:
Diámetro: 33 mm
Peso: 13,50 g
Calidad: Proof

ADEMÁS, DE REGALO, RECIBIRÁ UN PRÁCTICO EXPOSITOR AL ADQUIRIR 7 MONEDAS (***)

En el anverso se reproduce el escudo de la Capital o Ciudad Autónoma

(*) Aún disponibles.
(**) Precios válidos en el momento de la publicación del anuncio que podrán ser modificados en función de las cotizaciones de los metales.
(***) Para conseguir el expositor consulte las condiciones en el interior del estuche de cada moneda.

Reserve su colección en:

Tienda del Aeropuerto de Barajas-Madrid
Terminal 1, Zona No Schengen
Tel.: 91 305 55 29

La Tienda del Museo
Doctor Esquerdo, 36
28009 - Madrid
Tel.: 91 566 65 42
91 566 67 92
Fax: 91 566 66 96

Tienda on line:
www.fnmt.es/tienda

Julián Llorente
Espoz y Mina, 15
28012 - Madrid
Tel.: 91 531 08 41
Fax: 91 531 10 92

Lamas Bolaño
Gran Vía, 610
08007 - Barcelona
Tel.: 93 270 10 44
Fax: 93 302 18 47

Edifil
Bordadores, 8
28013 - Madrid
Tel.: 91 366 42 71
Fax: 91 366 48 21

Diputació, 305
08009 - Barcelona
Tel.: 93 487 02 00
Fax: 93 487 03 92

División de Venta a Distancia de El Corte Inglés
Tel.: 902 103 010

Estancos

Comercios Numismáticos y Filatélicos

Real Casa de la Moneda
Fábrica Nacional de Moneda y Timbre

www.fnmt.es/seriecapitales

II CONGRESO NACIONAL DE INTEROPERABILIDAD Y SEGURIDAD:

"Una administración más segura y conectada"

Organiza:

Club de Innovación

Con el apoyo de:

GOBIERNO DE ESPAÑA — MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS

Real Casa de la Moneda — Fábrica Nacional de Moneda y Timbre

FEMP — FEDERACION ESPAÑOLA DE MUNICIPIOS Y PROVINCIAS

GOBIERNO DE ESPAÑA — MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

CCN — Centro Criptológico Nacional

Patrocinador - Platino - :

Telefónica

Patrocinadores - Oro- :

gtt gestión tributaria territorial

GES CONSULTOR ens CUMPLIMIENTO INTEGRAL

Tecnocom

BlackBerry

VORTAL Connecting business.

indra

Santander

Colaboran:

Ingenia Ingeniería e Integración Avanzadas

T-Systems

nae

Deloitte.

athento

MIMACOM

MD TELECOMUNICACIONES

Bilbomática

software AG

Instituciones colaboradoras:

INTECO Instituto Nacional de Tecnologías de la Comunicación

IEEE TECHNOLOGY MANAGEMENT COUNCIL

FUNDACIÓN Astic

COSITAL Secretarios, Interventores y Tesoreros de Administración Local

Medios asociados:

cibersur

El Alcalde

REDES&TELECOM

computing

Revista Cloud Computing

gacetaTecnológica