19

LOS CRITERIOS DE SEGURIDAD, NORMALIZACIÓN Y CONSERVACIÓN COMO MARCO ORGANIZATIVO Y TÉCNICO PARA EL DESARROLLO DE LA ADMINISTRACIÓN ELECTRÓNICA

Francisco López Crespo
Jefe de Área de Sistemas Telemáticos
Ministerio de Administraciones Públicas. S.G. Coordinación de Recursos Tecnológicos de la A.G.E.

Miguel A. Amutio Gómez
Jefe de Área de Planificación y Explotación
Ministerio de Administraciones Públicas. S.G. Coordinación de Recursos Tecnológicos de la A.G.E.

Ricardo Cantabrana González
Técnico Superior Tecnologías de la Información
Ministerio de Administraciones Públicas. S.G. Coordinación de Recursos Tecnológicos de la A.G.E.

PRESENTACIÓN DE LOS CRITERIOS SNC

La Resolución de 26 de mayo de 2003, de la Secretaría de Estado para la Administración Pública, dispone la publicación del Acuerdo por el que se aprueban los Criterios de seguridad, normalización y conservación de las aplicaciones utilizadas por la Administración General del Estado (AGE) en el ejercicio de potestades (BOE 23-6-2003).

Los Criterios de seguridad, normalización y conservación (Criterios SNC) tienen como triple objetivo :

- Proporcionar el conjunto de medidas organizativas y técnicas (seguridad, normalización, conservación) que garanticen el cumplimiento de los requisitos legales para la validez y eficacia de los procedimientos administrativos de la Administración General del Estado, que utilicen los medios electrónicos, informáticos y telemáticos en el ejercicio de sus potestades.
- Facilitar la adopción generalizada por parte de la Administración General del Estado de medidas organizativas y técnicas que aseguren la protección proporcionada a los riesgos de los sistemas y aplicaciones que la manejan.
- Promover el máximo aprovechamiento de las tecnologías de la información y las comunicaciones en la actividad administrativa y asegurar a la vez el respeto de las garantías y derechos de los ciudadanos en sus relaciones con la Administración.

A lo largo de 168 páginas organizadas en 33 capítulos, distribuidos en 3 volúmenes, los Criterios SNC relacionan el marco legal con criterios técnicos[1].

- El marco legal. Requisitos relativos a la validez y eficacia de los procedimientos administrativos que utilicen los medios electrónicos informáticos y telemáticos, y de protección de los datos de carácter personal, entre otros.
- Con criterios técnicos. Organizativos o tecnológicos, basados en normas de autoridad y amplia aceptación.

Por otra parte, los Criterios SNC aportan:

- Recomendaciones que complementan a los criterios de forma obligatoria u opcional en función de la naturaleza de los datos y tratamientos o del nivel de protección exigible.
- Ampliación técnica con referencias a información en la que se fundamentan los criterios.
- Consideraciones que matizan el alcance o contenidos, tanto de los criterios como de las recomendaciones.
- Una relación de conceptos con explicación o definición de aspectos clave, para la clarificación y homogeneización de la terminología utilizada.
- Ejemplos de soluciones con algunas orientaciones de aplicación práctica.

MARCO LEGAL

Inicialmente, los Criterios SNC responden al mandato legal del *Real Decreto 263/1996 de 16 de febrero, por el que se regula la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado,* que encomienda al Consejo Superior de Informática y para el Impulso de la Administración Electrónica (CSI-AE) *"la aprobación y difusión de los criterios generales de seguridad, normalización y conservación de las aplicaciones" de "los programas y aplicaciones que efectúen tratamientos de información cuyo resultado sea*

utilizado para el ejercicio por los órganos y entidades del ámbito de la Administración General del Estado de las potestades que tienen atribuidas". Ampliado por el reciente Real Decreto 209/2003 por el que se regulan los registros y las notificaciones telemáticas, así como la utilización de medios telemáticos para la sustitución de la aportación de certificados por los ciudadanos.

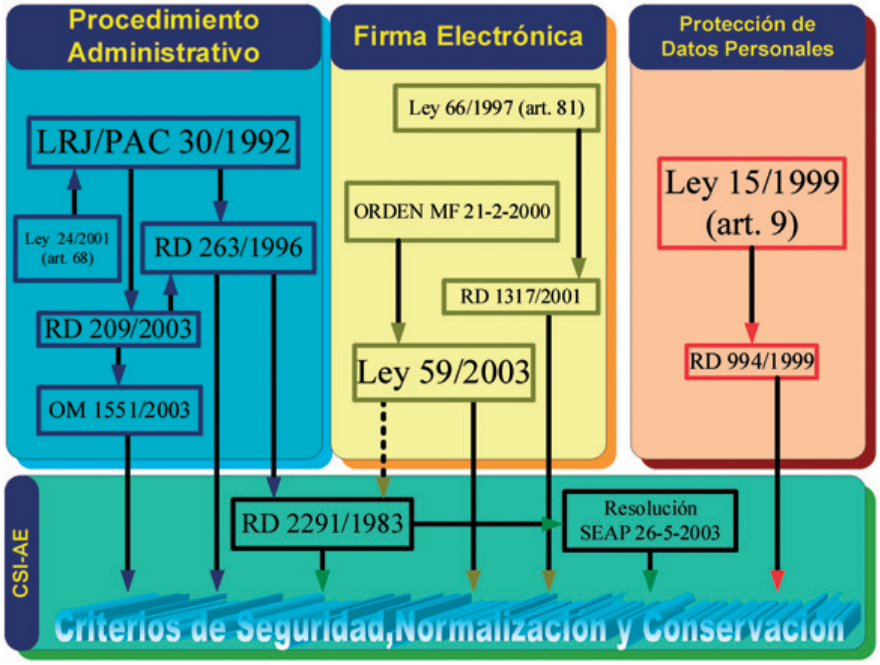

Ilustración 1. Relación del marco normativo estatal con los Criterios SNC

Ahora bien, no hubiera tenido sentido excluir otras disposiciones técnicas; de especial relevancia son las relativas a la protección de los datos de carácter personal, en particular, el *Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal*. Así mismo, se han contemplado las disposiciones relativas a la firma electrónica.

Las directrices del Programa IDA, de la Unión Europea, orientado a construir los servicios paneuropeos de Administración electrónica también han sido tomadas en cuenta en el desarrollo de los Criterios SNC.

CONTENIDO

Los Criterios SNC se estructuran en los volúmenes de seguridad, normalización y conservación, de los cuales se da una visión general a continuación:

Criterios de seguridad.

El volumen '*Criterios de seguridad*' expone los requisitos, criterios, y recomendaciones relativos a la implantación de las medidas de seguridad, tanto organizativas como técnicas, en el diseño,

desarrollo, implantación y explotación de las aplicaciones para el ejercicio de potestades. Evitando un enfoque fragmentario, aborda la seguridad con visión de conjunto. Incluye la protección de los datos de carácter personal al tener en cuenta los requisitos establecidos en la *Ley Orgánica 15/1999 de Protección de datos de carácter personal y en el citado Real Decreto 994/1999*.

Las aplicaciones para el ejercicio de potestades, así como la información que manejan y especialmente los datos de carácter personal, deben ser protegidas contra el menoscabo de sus propiedades de autenticidad, confidencialidad, integridad y disponibilidad. Al objeto de conseguir la protección adecuada, es necesario implantar un conjunto proporcionado de medidas de seguridad, tanto técnicas como organizativas, que permitan la creación de un entorno seguro para los servicios, la información, las aplicaciones y los sistemas que sustentan a todos ellos. Estas medidas organizativas y técnicas permitirán, en líneas generales, lo siguiente:

- Identificar, autenticar y, en su caso, autorizar el acceso a los sistemas de información.
- Identificar fidedignamente a remitente y destinatario de las comunicaciones electrónicas.
- Controlar el acceso para restringir la utilización, y el acceso a datos e informaciones, a las personas autorizadas y proteger los procesos informáticos frente a manipulaciones no autorizadas.
- Mantener la integridad de la información, y de los elementos del sistema, para prevenir alteraciones o pérdidas de los datos e informaciones.
- Garantizar la disponibilidad de la información y de las aplicaciones.
- Prevenir la interceptación, alteración y acceso no autorizado a la información.
- Gestionar las incidencias de seguridad.
- Auditar y controlar la seguridad.

Los Criterios de seguridad se estructuran en los siguientes 19 capítulos, además de la introducción:

2. Gestión global de la seguridad de la información
3. Política de seguridad
4. Organización y planificación de la seguridad
5. Análisis y gestión de riesgos
6. Identificación y clasificación de activos a proteger
7. Aspectos de seguridad ligados al personal
8. Seguridad física
9. Autenticación
10. Confidencialidad
11. Integridad
12. Disponibilidad
13. Control de acceso
14. Acceso a través de redes
15. Firma electrónica
16. Protección de soportes de información y copias de respaldo
17. Desarrollo y explotación de sistemas
18. Gestión y registro de incidencias

19. Plan de contingencias
20. Auditoría y control de la seguridad

El siguiente esquema presenta las relaciones funcionales que existen entre los diferentes capítulos del volumen de seguridad:

Ilustración 2. Relación entre los capítulos de seguridad

Estos contenidos utilizados conjuntamente con Magerit configuran a su vez un escenario de acciones, referencias y productos como el que se muestra en la figura siguiente:

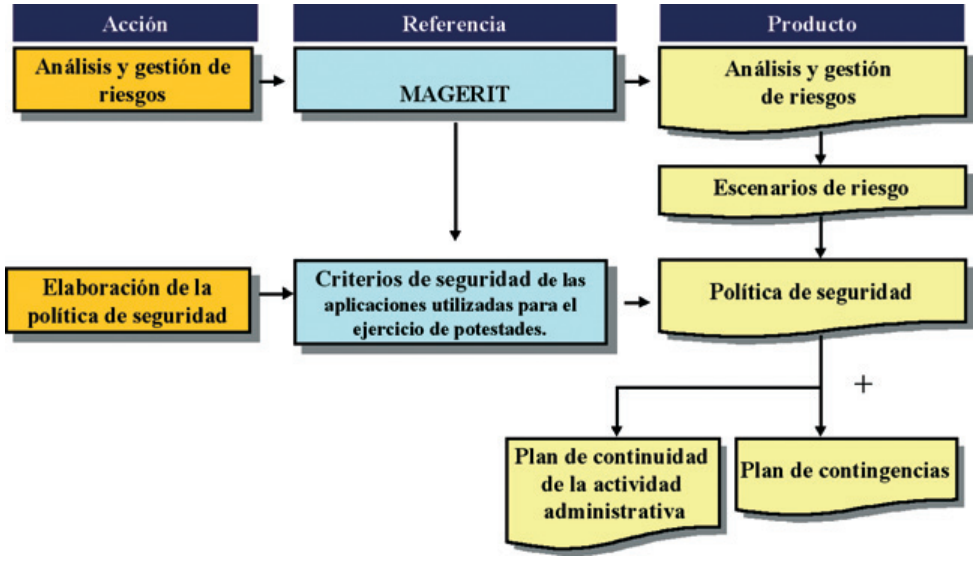

Ilustración 3. Utilización conjunta con MAGERIT

Los criterios y recomendaciones incluidos en este documento tienen presente las fuentes de autoridad en la materia y, en particular, que la *Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones sobre seguridad de las redes y de la información: Propuesta para un enfoque político europeo* insta a los Estados miembros a fomentar el uso de mejores prácticas

basadas en instrumentos existentes, tales como la norma UNE ISO/IEC 17799 '*Código de buenas prácticas para la gestión de la seguridad de la información*', que constituye un término de referencia fundamental de los criterios y recomendaciones incluidos en este documento. Así mismo se incluye como recomendación la utilización de productos y sistemas cuya seguridad haya sido certificada conforme a la norma ISO/IEC 15408 **"Common Criteria".**

Criterios de normalización.

El volumen '*Criterios de normalización*' expone las pautas para la normalización en los servicios electrónicos prestados por los órganos y entidades del ámbito de la Administración General del Estado con el objeto de facilitar la compatibilidad técnica, la disponibilidad y la interoperabilidad.

Tiene como objetivo fundamental facilitar el máximo aprovechamiento de las tecnologías de la información y las comunicaciones en la actividad administrativa en condiciones de racionalidad y economía, mediante la adopción de normas que aseguran la interoperabilidad de los sistemas informáticos y telemáticos.

Las aplicaciones utilizadas para el ejercicio de potestades deben poder desplegarse en un entorno que facilite la interoperabilidad de los siguientes elementos:

- Infraestructuras
- Servicios
- Contenidos
- Accesibilidad

Es habitual presentar estos elementos según un modelo conceptual de pirámide; sin embargo, la experiencia demuestra que su comportamiento práctico responde al principio de la cadena, de forma que cualquier obstáculo a la interoperabilidad, en cualquiera de los eslabones, afecta negativamente a la posibilidad de despliegue de la aplicación y de la prestación del servicio correspondiente.

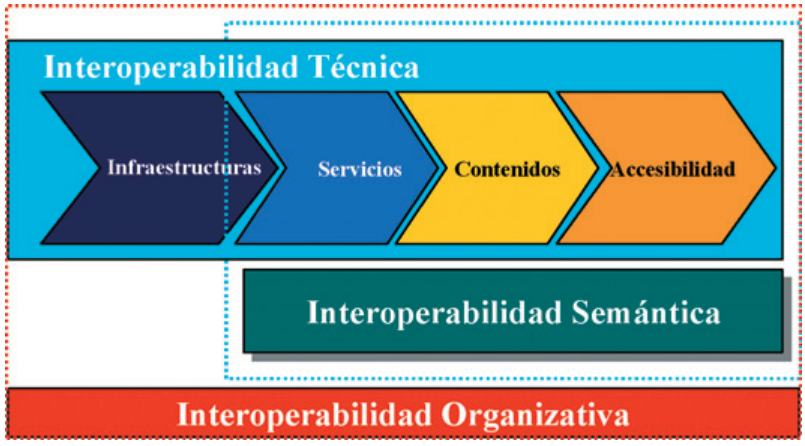

Ilustración 4. La cadena de la interoperabilidad

Aunque el ámbito de las cuestiones que llega a afectar a la interoperabilidad es muy extenso, pues alcanza incluso aspectos organizativos y semánticos, el acuerdo sobre un conjunto de

normas la facilita y se configura como el elemento clave de la racionalidad técnica y económica ya que su presencia es la que permite que el despliegue de las aplicaciones se pueda realizar de forma más rápida, más flexible y con menor coste.

Este acuerdo sobre un conjunto de normas es necesario pues a menudo se demuestra que la acción independiente de los diversos actores sectoriales no conduce, de forma espontánea, a un escenario de economías de escala o de racionalidad técnica que favorezca la integración y la interoperabilidad, dado que éstos tienden habitualmente a soluciones particulares *ad hoc*.

Es evidente, no obstante, que las normas por sí solas no garantizan que los procesos sean completamente independientes de las plataformas tecnológicas, sin embargo, la referencia a normas de autoridad es condición necesaria para la interoperabilidad. El reconocimiento de este hecho, se manifiesta en que la cuestión de la interoperabilidad ha saltado a un papel protagonista en el desarrollo de la Administración electrónica. Así el Plan de Acción *eEurope* 2005 incluye en relación con la *Administración en línea* una acción específica para el desarrollo de un marco de interoperabilidad que facilite la prestación de los servicios paneuropeos de administración electrónica a ciudadanos y empresas; tarea que se encomienda al Programa IDA.

La interoperabilidad figura así mismo entre las conclusiones de la Declaración Ministerial de Como (Italia, 7 y 8 de julio de 2003). Y constituye también el objeto del documento de trabajo de de la Comisión (*Linking up Europe: the importance of interoperability for e-government services*) que recoge el carácter estratégico de la interoperabilidad, desde los puntos de vista económico y técnico, como elemento esencial para el desarrollo de los servicios de Administración Electrónica a los niveles paneuropeo y nacional (central, regional y local) en un escenario donde no se produzcan 'islas' en la prestación de los servicios, para compartir y reutilizar la información y para la prestación de los servicios y difusión de la información administrativa a través de múltiples canales. Cabe destacar que en este documento se hace referencia explicita a los Criterios SNC como uno de los ejemplos llevados a cabo por Estados Miembros en materia de interoperabilidad.

Finalmente, diversos países de nuestro entorno (Reino Unido, Francia y Alemania, entre otros) vienen desarrollando desde hace algún tiempo las denominadas infraestructuras de interoperabilidad para facilitar el establecimiento de los servicios Administración-Ciudadano, Administración-Empresa y Administración-Administración.

El volumen de Criterios de normalización se estructura en los siguientes capítulos:

2. Presentación.
3. Interoperabilidad.
4. Metadatos.
5. Desarrollo de sistemas de información.
6. Requisitos de diseño de páginas web y de accesibilidad para personas con discapacidad.
7. Software libre y de fuente abierta.

En relación con las cuestiones que se tratan se recogen

- *Criterios.* Que señalan las normas que se deben adoptar y que se numeran para facilitar su localización y referencia:
- Normas aplicables. Con la remisión a referencias concretas.
- Consideraciones. Con explicaciones o matizaciones sobre el alcance o contenidos
- Ampliación técnica. Con referencias para ampliar y profundizar en las normas y conceptos técnicos.

Criterios de conservación

El volumen '*Criterios de conservación*' expone los requisitos, criterios y recomendaciones para la conservación de la información en soporte electrónico en las aplicaciones para el ejercicio de potestades.

La conservación de la información no debe considerarse de forma aislada; junto con la utilización y acceso a la información, es una etapa más del ciclo de vida de la misma en soporte electrónico. La gestión de dispositivos, soportes electrónicos y formatos debe ponerse en práctica aplicando procedimientos orientados a la manipulación de datos sensibles, especialmente si son de carácter personal; a la salvaguarda frente al deterioro, daño, robo o acceso no autorizado; a la eliminación o destrucción de soportes; a la gestión de los soportes removibles, etc. Estas medidas para la conservación de la información deben adoptarse de acuerdo con los especialistas en la gestión de archivos para diseñar soluciones prácticas a la medida de sus necesidades.

Los Criterios de conservación se estructuran en los siguientes capítulos:

1. Conservación de la información en soporte electrónico.
2. Ciclo de vida de la información en soporte electrónico.
3. Formato de la información en soporte electrónico.
4. Soportes.
5. Medidas de almacenamiento y conservación.
6. Sistema de archivos.

Los criterios y recomendaciones incluidos en este documento tienen en cuenta términos de referencia ampliamente aceptados y difundidos como la *Guía de la información electrónica* elaborada por el DLM Forum; en particular, recogen de esta fuente el modelo del ciclo de vida de la información en soporte electrónico que se muestra en el gráfico siguiente:

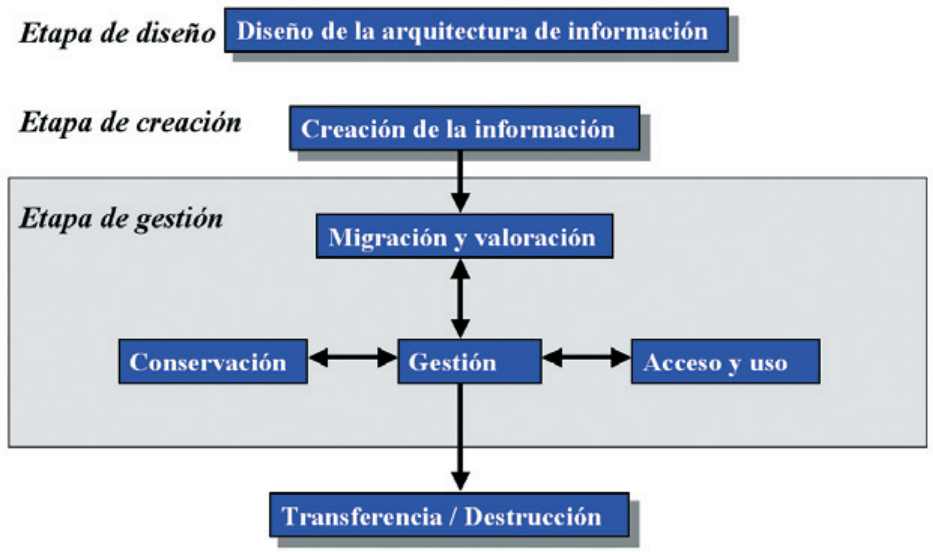

Ilustración 5. Ciclo de vida de la información electrónica

Valor añadido. Otras utilidades de los Criterios SNC

Además del cumplimiento del marco legal, el conocimiento de los Criterios SNC puede facilitar a los directivos, técnicos y usuarios, la adopción de las medidas proporcionadas a cada situación y contribuir a promover una mejor armonización y aprovechamiento de las tecnologías de la información y las comunicaciones en la actividad administrativa. En este sentido es explícita la estrecha relación entre los Criterios SNC y la metodología MAGERIT, de Análisis y Gestión de Riesgos de la Seguridad de la Tecnología de la Información, en particular en la determinación de las salvaguardas.

Los Criterios SNC presentan un gran conjunto de aspectos positivos para el impulso del desarrollo de la administración electrónica, entre ellos se pueden destacar los siguientes:

- Compilación racional y fácil de utilizar de las relaciones entre requisitos legales y normas técnicas de autoridad, tecnológicas y organizativas.
- Garantía del cumplimiento de legalidad.
- Lenguaje común para referirse a las aplicaciones en el ejercicio de potestades.
- Conjunto de buenas prácticas del ejercicio profesional.
- Racionalidad que facilita concentrar los esfuerzos en la tarea propia de cada uno, lo que repercute en la eficacia y productividad.
- Orientación a la empresa y la industria del sector de los requisitos de la Administración en términos de normas del mercado.
- Garantía de interoperabilidad entre los sistemas, con proyección de un futuro sin sobresaltos.
- Economía en el desarrollo y en el mantenimiento de los sistemas y en la formación de los recursos humanos.
- Confianza de los ciudadanos, quienes conocen los fundamentos de la protección de los datos y de los tratamientos
- Evolución y perfeccionamiento transparente y abierto a todos los profesionales y a las novedades legislativas o técnicas.

FUENTES DE EVOLUCIÓN

Los Criterios SNC, deben adaptarse y evolucionar con el fin de adecuarse, de forma eficiente, al entorno en el cual son utilizados. En concreto, los Criterios SNC, deben asimilar tanto las nuevas tendencias tecnológicas como los cambios que surjan en la normativa en la que se sustenta el ejercicio telemático de potestades. Por todo esto coexisten dos vías diferentes que imponen necesidades constantes de actualización:

- La evolución natural e independiente del producto a través de actualizaciones programadas y revisión de modificaciones devenidas del desarrollo de otros proyectos nacionales relacionados con administración electrónica
- La evolución derivada del marco internacional en el que participa el estado español que requiere adaptaciones e integración dentro de la política tecnológica tanto comunitaria como extracomunitaria.

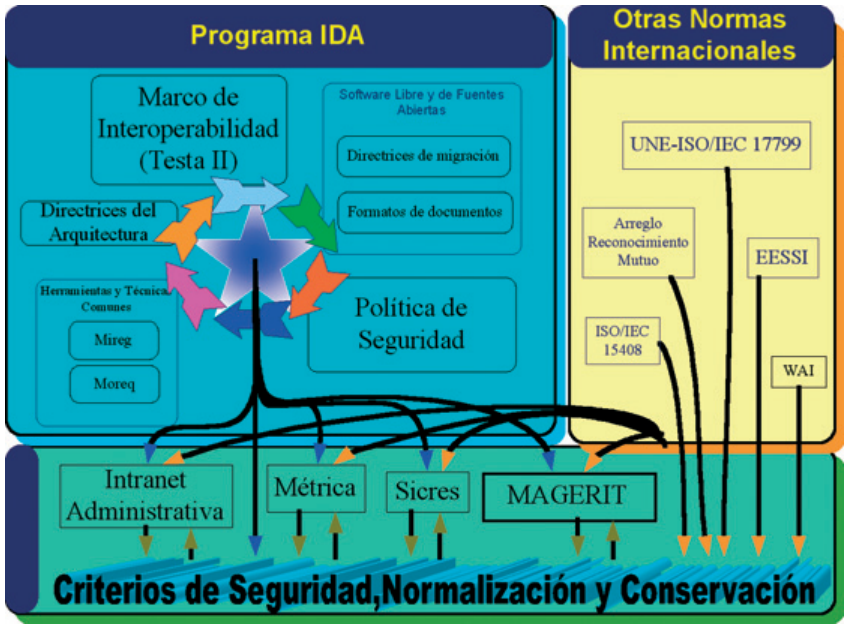

Ilustración 6. Relación de los Criterios SNC con otros programas e iniciativas

El grafico muestra la relación e influencias de las principales normas y programas técnicos nacionales e internacionales sobre los Criterios SNC.

Evolución como producto

Dentro del desarrollo de los Criterios SNC están programadas revisiones periódicas del contenido con el objetivo incluir las últimas tendencias y desarrollos tecnológicos y la normativa referente que vaya siendo elaborada por los departamentos legales. Así mismo se incorporan las observaciones y sugerencias que se hayan recibido por parte de los usuarios de los Criterios SNC.

En la actualización periódica realizada en el mes de junio se incluyen, entre otros cambios, la actualización del capítulo 15 ' Firma electrónica' adaptándose a los contenidos publicados en la Orden PRE 1551/2003 y en la Ley 59/2003 de firma electrónica. Así mismo se ha actualizado conforme a las previsiones de eEurope 2005 en materia del Marco Europeo de Interoperabilidad. Destacar un mayor protagonismo de la Intranet Administrativa dentro de los Criterios de Normalización y la actualización de las principales secciones del capitulo sexto, "Software Libre y de Fuentes Abiertas", perfeccionándose los criterios existentes en esta materia. Por último cabe mencionar las modificaciones en el apartado de conservación incluyéndose la referencia al formato ".sxw" de OpenOffice.org y la buena práctica de publicación de los documentos en diferentes formatos electrónicos alternativos.

Desde el CSI-AE, así como desde otros departamentos y administraciones, se están llevando a cabo diferentes iniciativas de fomento de la utilización de las tecnologías tanto dentro de las administraciones como en las relaciones de estas entre sí y con los ciudadanos.

Estas iniciativas constan, por ejemplo, de elementos como una **nueva versión de Magerit,** la versión 2. Esta metodología esta ligada íntimamente con el volumen de seguridad de los Crite-

rios SNC por lo que, simultáneamente, se esta realizando un alineamiento detallado entre ambos desarrollos con el fin de que exista una cohesión entre estas dos herramientas complementarias entre si.

También esta en fase de realización un paralelismo con el **Real Decreto 994/1999,** de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.

Por último se esta estudiando la posibilidad de un **enriquecimiento de los criterios,** incrementando el nivel de profundidad de los mismos y tratando de concretar de forma aún más técnica y específica aquellos puntos, y acciones, que puedan afectar tanto a la seguridad como a la interoperabilidad de los sistemas de información.

Evolución en el marco internacional

Dentro del marco internacional, los Criterios SNC han tomado como término de referencia a las **Directrices de Arquitectura IDA,** en las que se describen conceptos y referencias para la implantación de los servicios transeuropeos, tanto de los Proyectos de Interés Común como de las Acciones y Medidas Horizontales, al objeto de que sean construidos sobre una arquitectura común y bien definida. Por lo que ante cualquier evolución que sufran estas directrices deberá ser estudiada y traspuesta a los Criterios SNC

En referencia a los aspectos de seguridad, y de forma independiente al desarrollo nacional de Magerit, la Unión Europea establece, dentro del marco del programa IDA, la política de seguridad de IDA que contempla que los sistemas transeuropeos tienen condicionantes tales como el cumplimiento de la normativa comunitaria de protección de datos y de manejo de documentos oficiales clasificados. En su mayoría, estos condicionantes son aplicables a las infraestructuras de los Estados Miembros, tanto en su actividad independiente como integrada en las infraestructuras de la unión, por lo que la traslación de esta política al marco de los Criterios SNC colabora a prevenir dificultades en la seguridad, fiabilidad e interoperabilidad de los servicios elaborados por la administración.

Con el fin de integrar los criterios de seguridad en el marco mas amplio de normativa internacional referida a este campo se esta realizando una correspondencia con la norma **UNE-ISO/IEC 17799, Código de buenas prácticas para la Gestión de la Seguridad de la Información,** norma que, junto a ISO/IEC 15408 "*Common Criteria*", fue tomada como referencia en el desarrollo de los Criterios SNC.

Con respecto a la certificación electrónica, la vinculación la Iniciativa Europea de Normalización de la Firma Electrónica (EESSI) se hace patente al incluir los Criterios SNC al incluir estos en el capítulo 15 del volumen de Criterios de Seguridad referencia explícita a la firma electrónica.

Dentro de las orientaciones y políticas tecnológicas de la Unión Europea en cuanto a normalización y conservación los Criterios SNC integran o hacen referencia a **las herramientas y técnicas comunes del programa IDA** referidas a interoperabilidad de contenido incluyendo aspectos como los estudios sobre ebXML, los metadatos sobre información de la Administración (MiReg) o el Modelo de requisitos para la gestión de documentos electrónicos de archivo (MoReq)

Asimismo los Criterios SNC se establecen como marco de interoperabilidad propio, o instrumento equivalente, del que dispone nuestro estado dentro del **El Marco Europeo de Interoperabilidad,** encomendado al Programa IDA por el Plan de Acción *eEurope* 2005, en el que se abor-

dan las políticas y especificaciones técnicas recomendadas para lograr la interoperabilidad organizativa, semántica y técnica a fin de poder combinar los sistemas de información de las administraciones de la UE.

También cabe destacar el respaldo por parte de los criterios al software de fuentes abiertas por lo que es lógica la relación existente con las **Directrices IDA de migración a software de fuentes abiertas,** cuyo objetivo principal es ayudar a decidir si se debe emprender la migración a software de fuentes abiertas y describir en lenguaje técnico cómo debiera llevarse adelante la migración. Así como el respaldo de las **recomendaciones relativas a la promoción de la utilización de los formatos abiertos de documentos.**

SITIOS Y PÁGINAS WEB DE INTERÉS

Los Criterios de seguridad, normalización y conservación de las aplicaciones utilizadas por la Administración General del Estado en el ejercicio de potestades se encuentran disponibles en texto completo en formatos *pdf* y *html* en el sitio *web* del Consejo Superior de Informática y para el Impulso de la Administración Electrónica (http://www.csi.map.es/csi/pg5c10.htm), en el que se invita a formular observaciones u sugerencias, que se tendrán en cuenta en las sucesivas actualizaciones.

Otros organismos, programas y elementos citados a lo largo de esta comunicación están accesibles desde la siguiente relación

- Sitio web del Consejo Superior de Informática y para el Impulso de la Administración Electrónica: La construcción de los servicios paneuropeos de Administración electrónica: el Programa IDA http://www.map.es/csi/pg3315.htm
- Sitio web del Programa IDA http://europa.eu.int/ISPO/ida
- IDA Architecture Guidelines http://europa.eu.int/ISPO/ida
- Marco Europeo de Interoperabilidad. (http://europa.eu.int/ISPO/ida/jsps/index.jsp?fuseAction=showDocument&documentID=2319&parent=chapter&preChapterID=0-17)
- Directrices IDA de migración a software de fuentes abiertas (http://europa.eu.int/ISPO/ida/jsps/index.jsp?fuseAction=showDocument&parent=news&documentID=2339)"
- Open Source Observatory (Observatorio del Software de Fuentes Abiertas) (http://europa.eu.int/ISPO/ida/oso)
- Modelo de Requisitos para la gestión de documentos electrónicos de archivo (Especificación MoReq) (http://www.csi.map.es/csi/pg5m52.htm)

BLIOGRAFÍA

1- No es exclusivo de nuestro país el establecer una relación entre los requisitos legales y las normas técnicas (tecnológicas y organizativas). Por ejemplo, una aproximación similar puede encontrarse en la Health Insurance Portability and Accountability Act (HIPAA) de la agencia federal de los EEUU; Centers for Medicare and Medicaid Service (CMS).