Normativa y certificación en la Nube

-cuál sirve para qué-

Iniciativa de

CSA ES cloud security SPAIN alliance SM

En colaboración con

isms forum spain

Normativa y certificación en la Nube

Estudio elaborado por el capítulo español de Cloud Security Alliance

Coordinador

Olof Sandstrom (Arsys)

Colaboradores

Mariano J. Benito (GMV)

Flora Egea (IBM)

Jorge Laredo (HP)

Diego Bueno (KPMG)

Xavier Vila (Caja de Ingenieros)

Índice

Introducción

En los últimos años el uso de servicios en la Nube ha crecido de una forma muy relevante y su potencial de crecimiento en los próximos años es enorme.

De forma paralela al aumento del uso de servicios prestados desde la Nube, han ido surgiendo diversos intentos de normalización y sistematización de estos servicios: desde esquemas de certificación a códigos de buenas prácticas hasta el establecimiento de marcos regulatorios por diversos reguladores. Estos elementos pretenden aportar criterios sólidos y consistentes de funcionalidad, seguridad e interoperabilidad en los segmentos de proveedor y cliente.

Desde el capitulo español de Cloud Security Alliance (en adelante CSA-ES) hemos considerado oportuno realizar una revisión de estas normas, códigos de buenas prácticas, etc. para poder resumir a los posibles usuarios de estos documentos en qué consiste cada uno, y cuál puede ser el interés para su organización.

La intención de CSA-ES es continuar con el desarrollo de este estudio en próximos años, manteniéndolo actualizado con las nuevas versiones de los documentos y referenciales considerados (ver Anexo XX), así como incorporando al estudio aquellos que se consideren relevantes. Esta consideración puede estar abierta a referenciales y/o cuerpos legislativos de otros países.

Metodología de trabajo

Para la realización del estudio, se realizó un Call for Volunteers entre miembros de CSA-ES y otros profesionales. Como resultado del mismo, se constituyó un equipo de trabajo, integrado por los autores del estudio y con el apoyo de ISMS Forum.

A continuación se establecieron criterios comparativos que permitan tanto a proveedores como clientes conocer las particularidades de cada uno de estos esquemas y códigos, de forma que puedan diferenciar claramente las particularidades de cada uno de ellos y conocer cuál o cuáles de ellos van a aportar mayor valor a estos actores en sus escenarios de aplicación.

Obviamente una parte fundamental del trabajo era la elección de los marcos de referencia que se iban a analizar. Esta tarea requirió de varias iteraciones, hasta que finalmente se consensuo una base de trabajo común.

Seguidamente se distribuyeron los marcos de referencia entre los miembros del grupo de trabajo, de forma que cada uno se encargaría de revisar un subconjunto, y hacer sus aportaciones.

Finalmente se ha realizado un trabajo de edición bastante relevante con el objeto de unificar todas las aportaciones sobre un único documento, consolidando no solo los contenidos, sino también los estilos.

Objetivo

El objetivo principal del informe es comparar los diferentes marcos de referencia (normas, códigos de buenas prácticas, guías, leyes, etc.) en materia de Computación en la Nube (o Cloud Computing) contra unos criterios comparativos comunes.

El resultado se articula en el establecimiento de criterios de comparación de cada uno de los referenciales incluidos en el análisis y la valoración efectiva de cada uno de los referenciales en base a los criterios anteriores para permitir su comparación tanto por proveedores como clientes, de forma que puedan diferenciar claramente las particularidades de cada uno de ellos y su aplicabilidad.

Se han establecido además diversos casos de uso en los que cada referencial es particularmente eficaz en su aplicación. Los casos de uso identificados (ver Capitulo XXX) son, a criterio del Grupo de Trabajo del Estudio, de particular interés, puesto que definen casuísticas habituales en el mercado, tanto por la parte proveedora como por la parte consumidora de servicios en la Nube. De esta forma, un lector de la presente taxonomía que se halle en uno de estos casos de uso dispone de una guía directamente aplicables de marcos de trabajo que le son aplicables.

Alcance

El presente estudio compara frente a unos criterios comunes los principales elementos de mayor difusión a nivel internacional, europeo y español.

Igualmente se han tomado en consideración aquellos marcos de referencia que, no entrando estrictamente dentro de los criterios establecidos en el alcance, el grupo de trabajo que ha elaborado este informe ha considerado especialmente relevantes.

Audiencia

Se pretende que este informe sea útil para proveedores y usuarios de servicios Servicios en Nube pública en sus tres vertientes de IaaS, PaaS y SaaS.

Asimismo puede servir de referencia a los proveedores y clientes de Nube Privada a la hora de acordar sus condiciones particulares.

Conclusiones

Tras realizar la revisión de los marcos de referencia, el grupo de trabajo ha llegado a las siguientes conclusiones:

1. Hay un número muy relevante de marcos de referencia aplicables al entorno de los servicios en la Nube. Probablemente ningún paradigma tecnológico o cambio haya generado un cuerpo normativo tan extenso en tan poco tiempo.
2. Una parte relevante de las normas y códigos de buenas prácticas que se aplican en el ámbito de los servicios en la Nube, no son específicos de la Nube. Tratan sobre ámbitos TIC de forma general, y las organizaciones lo adoptan para un entorno en la Nube.
3. En general, cada marco de referencia se han desarrollado de forma independiente, sin tomar en consideración de una forma significativa lo que otros marcos ya habían desarrollado.
4. Probablemente asistiremos a una consolidación de los marcos de referencia en función de la evolución de cada uno dentro del mercado, tras lo cual quedara un numero reducido de marcos de referencia de facto en cada área (sistemas, gestión, profesionales, etc.).
5. La protección de los datos personales en los servicios en la Nube, entendido como derecho fundamental en Europa, añade cierta complejidad al desarrollo de los marcos de referencia, especialmente en lo que atañe a la internacionalización de dichos marcos.

Criterios de Comparación

Para la elaboración del presente informe se han tomado en consideración los siguientes criterios de comparación.

- Tipo
  - Norma
  - Código de buenas prácticas
  - Recomendación
  - Cuerpo de conocimiento
  - Cuerpo legislativo o regulatorio
- Cumplimiento
  - Obligatorio
  - Voluntario
- Ámbito
  - España
  - Nacional otros países
  - Europeo
  - Internacional
- Alcance
  - Global
  - Especifico de producto
  - Especifico de servicio
  - Especifico de tecnología
- Sector
  - Global
  - Administración pública
  - Sector privado
- Orientación
  - Profesionales
  - Sistemas TIC
  - Procesos y procedimientos
  - Gobierno IT
- Certificación
  - Primera parte
  - Segunda parte
  - Tercera parte
- Aplicabilidad
  - Caso de uso 01 a 06. Según las descripciones anteriores

Marcos de referencia incluidos en el estudio

Legislación aplicable

- Esquema Nacional de Interoperabilidad
- Esquema Nacional de Seguridad
- Ley Orgánica de Protección de Datos de Carácter Personal
- Reglamento de Desarrollo de la LOPD

Certificaciones de sistema

- ISO 27001:2013 Information Security Management Systems, Requirements
- ISO 20000-1:2011 Service Management System, Requirements
- Cloud Security Alliance Open Certification Framework (CSA OCF)
- Cloud Security Alliance Security, Trust and Assurance Registry (CSA STAR)
- Eurocloud Star Audit
- Payment Card Industry Data Security Standard (PCI DSS)
- Statement on Standards for Attestation Engagements 16 SOC1, SOC2, SOC3 (SSAE 16 1-2-3)

Certificaciones profesionales

- Cloud Security Alliance Security, Certificate of Cloud Security Knowledge (CSA CCSK)
- Cloud Security Alliance Security, Certificate of Cloud Security Professional (CSA CCSP)

Códigos de buenas prácticas

- ISO 27002:2013 Code of practice for information security controls
- ISO 27018:2014 Code of practice for PII protection in public clouds acting as PII processors
- CSA Cloud Control Matrix
- Cloud Industry Forum Code Of Practice (CIF COP)

Guías de uso

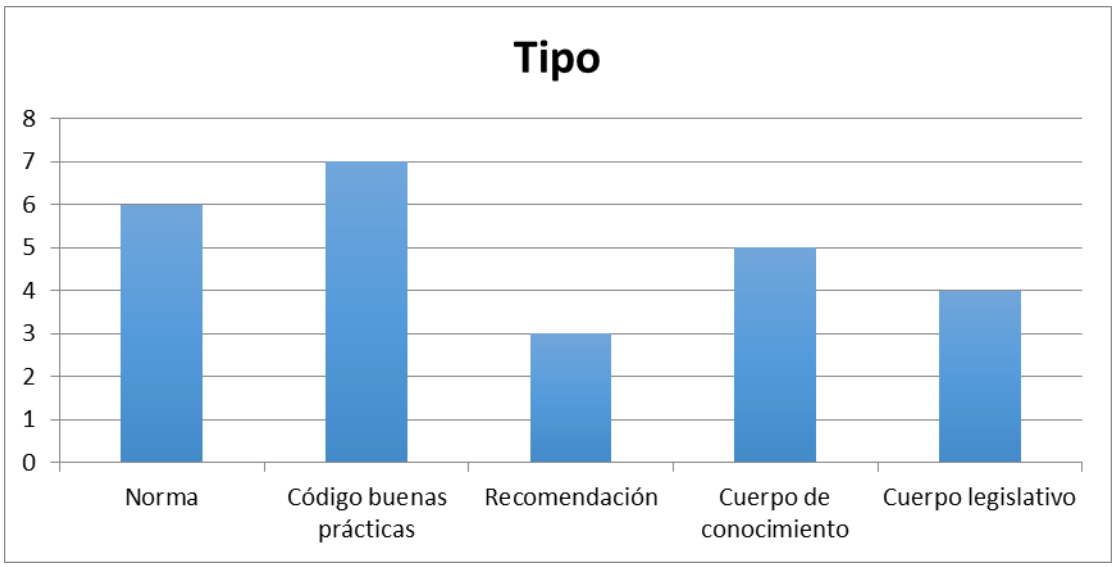
- CCN STIC 823 Guía de seguridad de las TIC, utilización de servicios en la nube
- Article 29 WP196
- Guía APD para clientes que contraten servicios de Cloud Computing
- Guía APD para prestadores de servicios de Cloud Computing

Taxonomía de los marcos de referencia incluidos

Actualmente existe un número relevante de marcos de referencia que pretenden, o se pueden utilizar para, normalizar, estandarizar o regular los servicios en la Nube, tanto desde el punto de vista de los proveedores de servicio, como de los profesionales del sector o de los clientes finales. En el presente estudio se han analizado un total de 22.

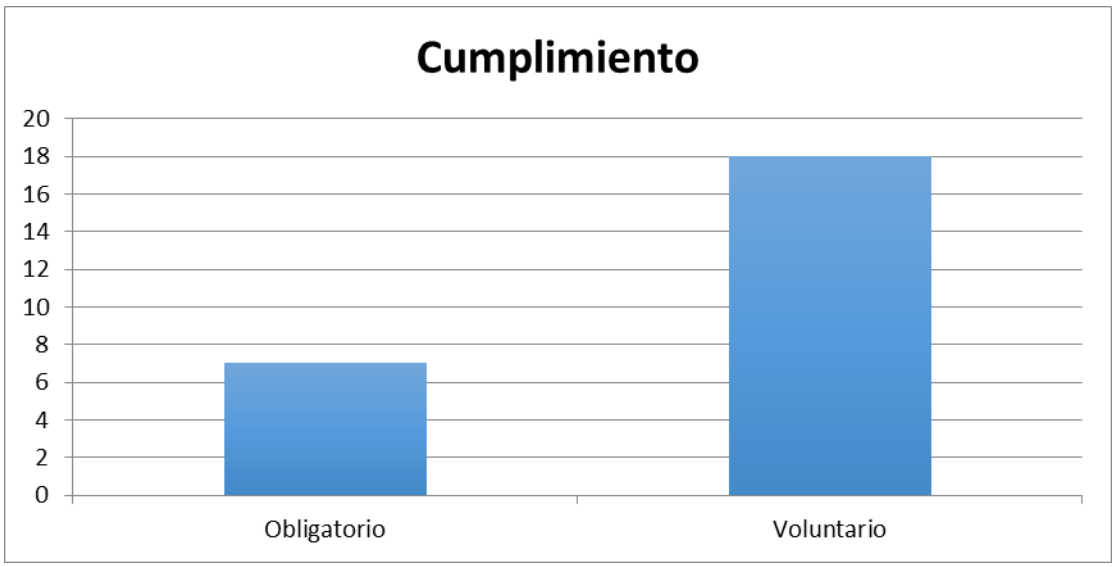
En lo referente al tipo de documento, hay una distribución bastante homogénea. Existe un número relevante de marcos de referencia cualquiera que sea el interés del usuario. El hecho de que tanto la industria como los usuarios hayan desarrollado un conjunto documental significativo en tan poco tiempo, se interpreta como:

- Una evidencia más del interés por los servicios en la Nube de todas las partes involucradas.
- Un reflejo de la amplitud e influencia de la Computación en la Nube en la prestación de servicios TI, que ha hecho que todas las organizaciones anteriores a la creación del paradigma hayan hecho "su estándar de Nube", con distintos enfoques. Este mismo comentario aplica a las respuestas dadas desde los gobiernos al campo, en un intento regulatorio.
- La inexistencia de una única aproximación a la estandarización de la Nube. Aún no está claro si será más eficaz la autorregulación, las buenas prácticas tecnológicas y profesionales, la emisión de leyes. Por ello, se están probando todas.



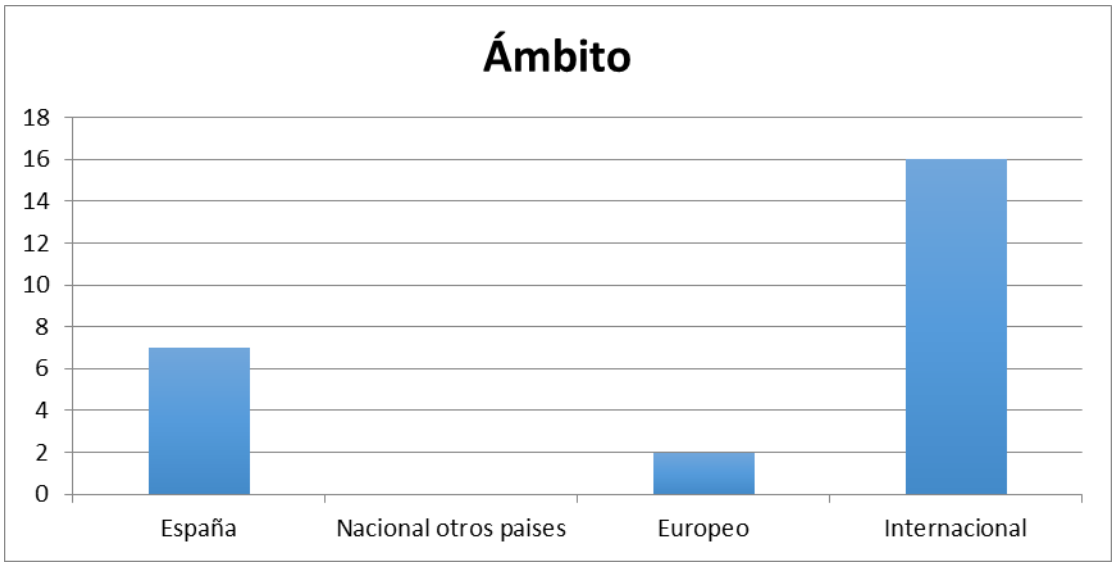
En cuanto a si su cumplimiento es obligatorio o no, se ha encontrado que fundamentalmente son de obligatorio cumplimiento los cuerpos legislativos, en algunos casos hay estándares de cumplimiento obligado para poder realizar determinadas actividades.

El caso más claro es la obligación de cumplir con la normativa PCI-DSS para poder gestionar datos de tarjetas de crédito. Pero la mayor parte de los estándares son voluntarios, reflejo de que en un ámbito de prestación global de los servicios, sólo una autoridad global y con capacidad de influenciar puede hacer obligatorio un estándar. El resto de intentos quedan como obligatorios a nivel local o regional, y como voluntarios para el resto de alcances.



El aspecto global de los servicios en la Nube se ha visto reflejado en los resultados, predominando los marcos de referencia cuyo ámbito de aplicación es internacional, es decir, que son de aplicación en cualquier país.

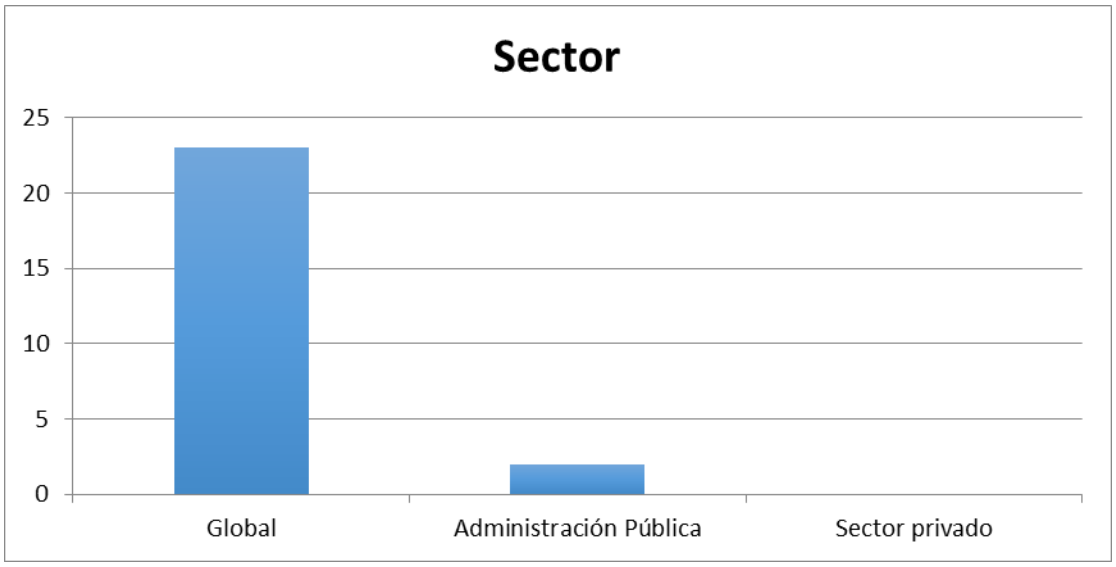
Al haber realizado el estudio en España, se han incluido una serie de marcos de referencia que son de aplicación únicamente en este país (LOPD, ENS, etc.). Probablemente en posteriores versiones del presente estudio sería interesante analizar otros marcos de referencia de aplicación exclusiva en otros ámbitos geográficos.



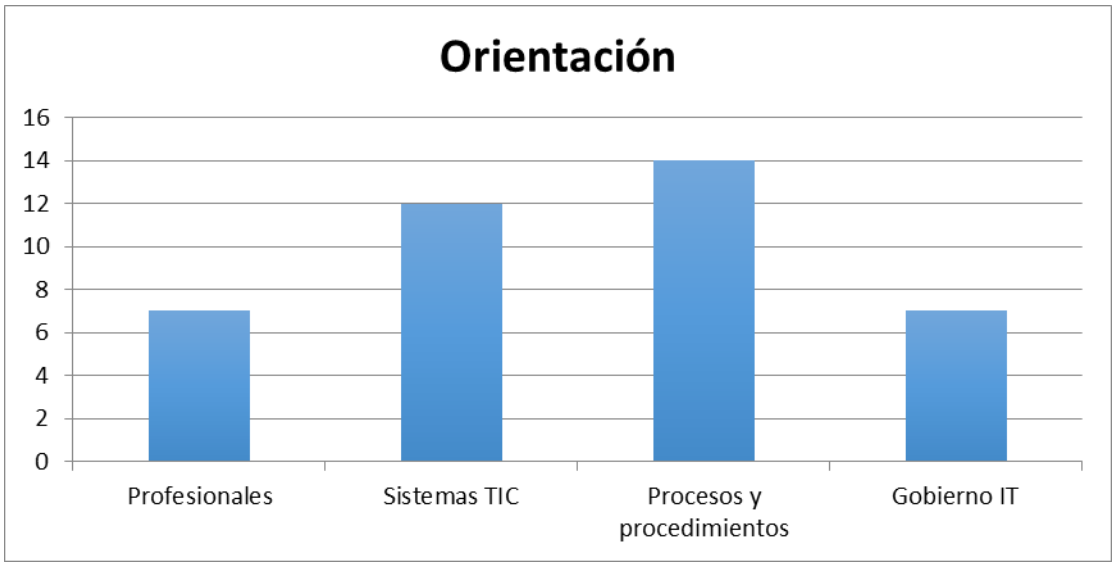
Aunque cuando se inició el estudio, el equipo tenía la percepción de que había un porcentaje relevante de marcos de referencia que eran de aplicación específicamente para un determinado producto, servicio o tecnología, lo cierto es que la mayoría de los marcos contemplados en el estudio tiene un alcance de aplicación global.

De forma similar a lo ocurrido en el estudio del alcance, el equipo creía que existía una frontera más o menos clara entre los referenciales que son de aplicación en el sector público y los que lo son en el sector privado. La cuestión que se ha encontrado tras analizarlos es que, dada la globalidad de los servicios prestados desde la Nube, prácticamente todos los marcos de referencia son de aplicación en ambos sectores. Igualmente los marcos de referencia específicos de una tecnología están asociados habitualmente a un fabricante concreto, como parte de su portfolio de formación de su producto a clientes y partners, y asociado a su portfolio de servicios en la Nube.

En cualquier caso, no se ha identificado un marco de referencia de función comparable a "Common Criteria para la Nube" que normalice cómo desarrollar servicios seguros en este entorno.

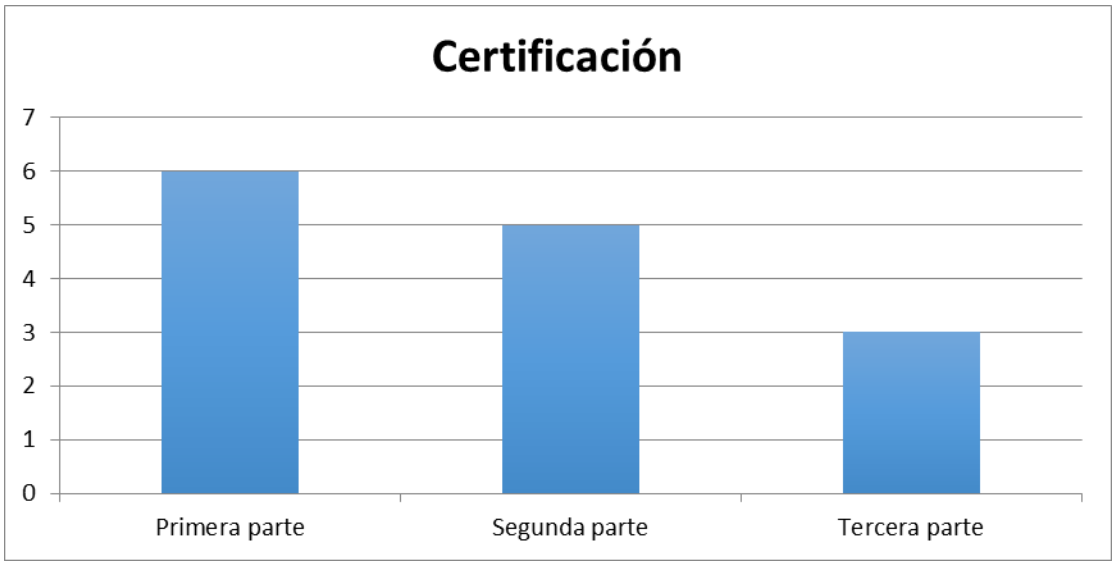


En lo que respecta a la orientación de los marcos de referencia, se ha apreciado una distribución bastante uniforme.



Probablemente la certificación sea uno de los aspectos relevantes del hecho de adoptar un determinado marco de referencia, pues permite a la organización o al profesional evidenciar unas capacidades determinadas en el ámbito de la Nube. Cuando se habla de que una entidad o un profesional cuenta con una certificación, habitualmente se entiende que se está haciendo referencia a una certificación de tercera parte de confianza.

Sin embargo en muchas ocasiones se trata de una certificación de segunda parte, que sin pretender restarle importancia, no ofrece las mismas garantías que la certificación de tercera parte. Los resultados del estudio indican que el porcentaje de marcos de referencia que permiten abordar una certificación de tercera parte es aún reducido.



El estudio de los diferentes marcos de referencia nos indica que la mayoría de los marcos de referencia son de aplicación para un caso de uso de un prestador de servicios, ya sea privado o público. Las diferencias se acentúan ligeramente en los casos de uso como clientes. En este sentido una de las conclusiones del estudio sería que son los casos de uso de los clientes los que determinan los marcos de referencia que deberían contemplar los proveedores de servicios en la Nube.

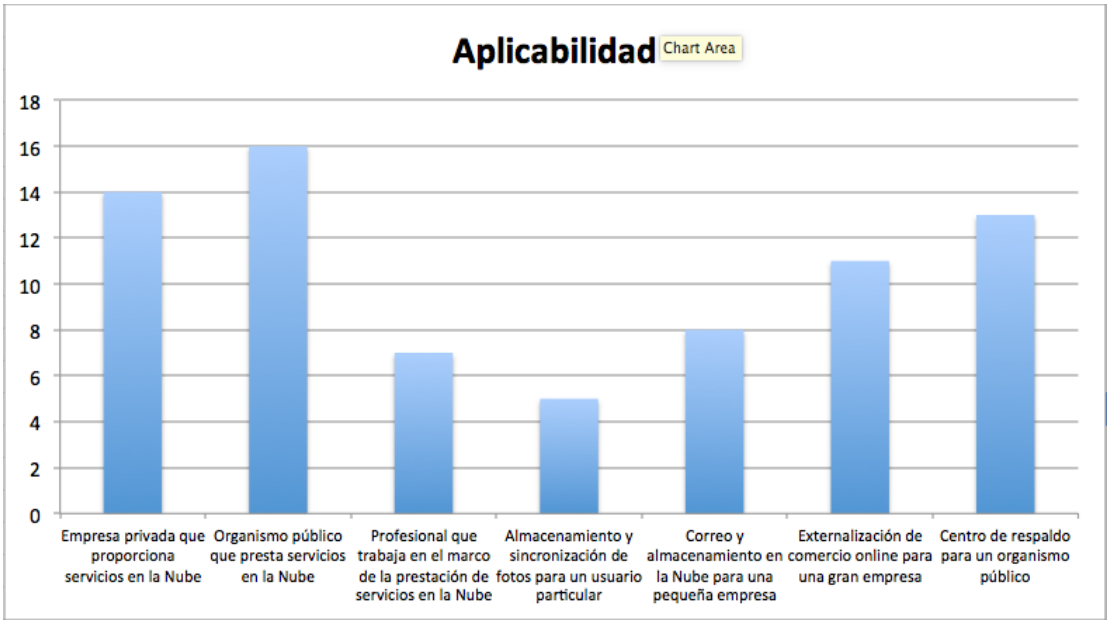


Tabla de Comparación de Marcos de Referencia

Criterios objetivos de comparacion		Tipo				Cumplimiento		Ámbito				Alcance				Sector		Orientación			Certificación			Aplicabilidad					
		Norma	Código buenas prácticas	Recomendación	Cuerpo de conocimiento	Cuerpo legislativo	Obligatorio	Voluntario	España	Nacional otros países	Europeo	Internacional	Global	Específico producto	Específico servicio	Específico tecnología	Global	Administración Pública	Sector privado	Profesionales	Sistemas TIC	Procesos y procedimientos	Gobierno IT	Primera parte	Segunda parte	Tercera parte	Caso de uso 01	Caso de uso 02	Caso de uso 03	Caso de uso 11	Caso de uso 12	Caso de uso 13	Caso de uso 14
Legislación	ENI					x	x		x				x				x	x			x	x	x				x	x				x
	ENS					x	x		x				x				x	x			x	x	x	x			x	x				x
	LOPD					x	x		x				x				x				x	x	x				x	x				x
	RMS					x	x		x				x				x				x	x	x				x	x				x
	REPD	x					x				x		x				x															
Certificación de sistema	ISO 27001	x						x				x	x				x				x	x				x	x					x
	ISO 20000-1	x						x				x	x				x					x				x	x					x
	CSA OCF		x					x				x	x				x									x	x					x
	CSA STAR		x					x				x	x				x									x	x					x
	ECSA		x					x			x		x				x							x			x					x
	PCI DSS	x					x					x	x				x			x			x			x					x	
	SSAE 16	x					x					x	x				x															
Certificación profesional	CSA CCSK				x			x				x	x			x	x			x								x					
	CSA CCSP				x			x				x	x			x	x			x													
Código buenas prácticas	ISO 27002		x					x				x	x				x					x	x				x					x
	ISO 27018	x						x				x	x				x						x				x					x
	CSA CCM		x					x				x	x				x			x												
	CIF COP		x					x				x	x				x						x	x			x					x
Guía de uso	CCN STIC 823		x					x	x				x		x		x						x	x			x	x				x
	Article 29 WP196			x				x			x		x				x						x				x	x				x
	Guia APD Clientes Cloud			x				x		x			x				x						x				x	x				x
	Guia APD Proveedores Cloud			x				x		x			x				x						x				x	x				

Casos de uso

En el marco de la elaboración del presente informe se han considerado los siguientes casos de uso en los que se considera que las conclusiones del estudio pueden ser de utilidad.

Segmento proveedor

01 Empresa privada que proporciona servicios en la Nube

Un proveedor de servicios en la Nube ha detectado últimamente una mayor reticencia en el mercado a contratar sus servicios frente a los de su competencia. Uno de los argumentos que alega su equipo comercial es que su competencia dispone de las certificaciones adecuadas y ellos no.

Su objetivo es determinar qué certificación le proporcionaría un mejor posicionamiento en el mercado.

02 Organismo público que presta servicios en la Nube

Un organismo público es el encargado de prestar servicios en la Nube tanto a una serie de organismos públicos relacionados, como a los ciudadanos en su calidad de clientes finales de los mismos.

Como prestador de servicios en la Nube quiere mejorar su nivel interno de seguridad, reduciendo así la probabilidad de que se produzcan incidentes, el potencial impacto de los mismos, y por tanto el nivel de riesgo.

Su objetivo es determinar qué certificación le proporcionaría el marco general más adecuado para mejorar la seguridad de los servicios que presta.

03 Profesional que trabaja en el marco de la prestación de servicios en la Nube

Un administrador de sistemas senior lleva trabajando ya un tiempo con entornos en la Nube, especializándose en las tareas relacionadas con la securización de este tipo de entornos. Sin embargo no dispone de una certificación profesional que evidencie su perfil como experto en seguridad sobre estas tecnologías.

Su objetivo es determinar qué certificación es la mejor valorada en el mercado laboral para evidenciar sus conocimientos profesionales.

Segmento cliente

11 Almacenamiento y sincronización de fotos para un usuario particular

Un particular quiere utilizar servicios básicos en la Nube para almacenar en remoto las fotos y/o videos que saca con su dispositivo móvil.

Su objetivo es contar con un servicio gratuito de forma que sus fotos se puedan sincronizar con el resto de sus dispositivos.

Desea contratar un servicio que cubra sus necesidades funcionales, sencillo de usar y que le proporcione un nivel de confianza suficiente de que sus fotos no van a ser accesibles por personas no autorizadas.

Para seleccionar adecuadamente un proveedor de servicios, desea saber que cláusulas deberían estar presentes en los términos y condiciones del proveedor, y si tiene sentido o no que disponga de algún tipo de certificación.

12 Correo y almacenamiento en la Nube para una pequeña empresa

Una pequeña empresa quiere utilizar servicios básicos en la Nube para su correo electrónico y agenda, compartir documentos y guardar una segunda copia de seguridad en un emplazamiento distinto al de sus propias instalaciones.

Su objetivo es reducir la dependencia de personal o externos que gestionen la informática, reduciendo los costes si es posible.

Desea contratar un servicio que cubra sus necesidades funcionales, sencillo de usar y que le proporcione un nivel de confianza suficiente de que sus correos y documentos van a estar disponibles y que no van a ser accesibles por personas no autorizadas.

Para seleccionar adecuadamente un proveedor de servicios, desea saber qué normativas o certificaciones debería tener.

13 Externalización de comercio online para una gran empresa

Una gran empresa quiere utilizar servicios en la Nube para externalizar su comercio online, que actualmente está hospedado en su centro de proceso de datos y operado por su departamento de TI.

Su objetivo es mejorar la disponibilidad actual de su plataforma, reducir los costes de personal de TI y reducir los costes de explotación.

Desea contratar un servicio que cubra sus necesidades funcionales, que incluya servicios de administración y soporte técnico, le garantice el cumplimiento con los requerimientos legales de su plataforma. Igualmente debe proporcionarle un nivel de seguridad consistente con la importancia que tiene para la empresa la integridad de los datos de sus transacciones online, así como la confidencialidad de los mismos.

Desea saber con qué normativas o certificaciones debería contar un proveedor, para recogerlo como un requerimiento más dentro de su documento de solicitud de ofertas.

14 Centro de respaldo para un organismo público

Un organismo público quiere utilizar servicios en la Nube como parte de su plan de continuidad de negocio, de forma que pueda levantar determinados servicios en un centro remoto en caso de que se produzca una incidencia en su centro principal.

Su objetivo es migrar su actual centro de continuidad de negocio basado en tecnología tradicional, subcontratando su gestión y operación basándose en tecnologías y serviciosen la Nube. Con ello pretende mejorar la eficacia de su plan de continuidad de negocio y reducir los costes relacionados con sus necesidades de continuidad.

Desea contratar un servicio que cubra sus necesidades funcionales, que incluya servicios de administración y soporte técnico, le garantice el cumplimiento con los requerimientos legales de su plataforma. Dada la naturaleza de los servicios contemplados dentro del plan de continuidad de negocio, debe proporcionarle un nivel de seguridad muy elevado.

Desea saber con qué normativas o certificaciones debería contar un proveedor, para recogerlo como un requerimiento más dentro de su pliego de prescripciones técnicas.

Estudio de los marcos de referencia

Esquema Nacional de Interoperabilidad

Nombre	Esquema Nacional de Interoperabilidad	**Extensión del documento**	18
Versión en vigor	Real Decreto 4/2010, de 8 de enero	**Gratuito**	Si
Organización que lo mantiene	Ministerio de la Presidencia, Gobierno de España	**Año de aprobación**	2010

Objetivo	La creación de las condiciones necesarias para garantizar el adecuado nivel de interoperabilidad técnica, semántica y organizativa de los sistemas y aplicaciones empleados por las Administraciones públicas, que permita el ejercicio de derechos y el cumplimiento de deberes a través del acceso electrónico a los servicios públicos, a la vez que redunda en beneficio de la eficacia y la eficiencia.
Observaciones	Hace foco en la reutilización segura de recursos por parte de la administración, de forma cualquier entidad pueda acceder a servicios, información, funciones u otros recursos compartidos por otra entidad de la Administración, con las debidas garantías de Calidad de Servicio, Calidad de Datos y Seguridad de la Información. La interoperabilidad ha de ser técnica, semántica y organizativa. De esta forma, el ENI persigue la optimización de los recursos dedicados por la Administración y la mejora de la Calidad del Servicio prestados al ciudadano. En sentido estricto, no tiene por qué tener un impacto en la prestación de servicios desde la Nube, más allá de ser requisitos que la Administración debería exigir a cualquier proveedor de servicios en la Nube (CSP según sus siglas en inglés) que quiera prestar servicios. Sin embargo, proporciona una definición muy completa de datos, servicios de certificación y firma y servicios disponibles, estandarizada y completa, y que es un requisito de un cliente con un volumen de negocio apreciable. La adopción del ENI por un CSP simplifica la tarea de implantación y adelanta el cumplimiento de los requisitos de cliente.

Esquema Nacional de Seguridad

Nombre	Esquema Nacional de Seguridad	**Extensión del documento**	25
Versión en vigor	RD 3/2010 del 8 de agosto modificado por RD 951/2015 de 23 de octubre	**Gratuito**	Si
Organización que lo mantiene	CNI	**Año de aprobación**	2010

Objetivo	El Esquema Nacional de Seguridad (RD 3/2010 del 8 de agosto) es una normativa de obligatorio cumplimiento para toda administración pública en referencia a la gestión de la seguridad de la información. Aún ser de obligado cumplimiento, no está muy implantada en la administración pública al no haber ninguna forma de sanción ni de forzar esta aplicación.
Observaciones	En relación a aspectos relacionados con la computación en la Nube, el propio CNI publicó un documento de recomendaciones de seguridad en la Nube. En este documento deja claro que la disponibilidad es responsabilidad del proveedor de servicios en la Nube, pero el resto de ámbitos (Integridad, Confidencialidad, Trazabilidad y Autenticidad) depende de lo que se haga y quién lo haga, por lo que solicita que se defina en el contrato de servicio. Marca unas recomendaciones según lo que esté en un nivel (bajo, medio o alto), actividades que no se deben hacer (misma máquina base, registros diferenciados, ...). Desarrollado posteriormente y en detalle en la SITC-823.

Ley Orgánica de Protección de Datos

Nombre	Ley Orgánica de Protección de Datos de Carácter Personal	**Extensión del documento**	12 (BOE)
Versión en vigor	Ley Orgánica 11/1999 de 13 de diciembre	**Gratuito**	Si
Organización que lo mantiene	Congreso de los Diputados Agencia Española de Protección de Datos	**Año de aprobación**	1999

Objetivo	Regula la protección de datos personales en España. Es una trasposición de la Directiva Europea 95/46/CE del 24 de octubre de 1995
Observaciones	El Tribunal Constitucional en su sentencia STC 292 de 30/11/2000 declaro nulos parte de los artículos 21 y 24. Las medidas de seguridad y otros aspectos están desarrollados en detalle en su Reglamento de desarrollo aprobado mediante el Real Decreto 1720/2007. En lo que respecta a las transferencias internacionales de datos se ha de tener en cuenta los efectos de que el Tribunal Superior de Justicia Europeo haya declarado inválido el Acuerdo 'Safe Harbor' con los Estados Unidos. Las transferencias de datos personales a Estados Unidos se han de revisar en base a esa sentencia si bien está en fase de clarificación cuáles serán sus efectos. Está previsto en un futuro su sustitución por el Reglamento Europeo de Protección de datos. La LOPD permite el tratamiento de datos por cuenta del responsable del fichero definiendo la figura de Encargado del tratamiento y definiendo una serie de obligaciones del Responsable y del Encargado.

Reglamento de Desarrollo de la LOPD

Nombre	Reglamento de desarrollo de la LOPD
Versión en vigor	Real Decreto 1720/2007, de 21 de diciembre
Organización que lo mantiene	Gobierno de España Agencia Española de Protección de Datos

Extensión del documento	34 (BOE)
Gratuito	Si
Año de aprobación	2007

Objetivo	El reglamento tiene como objeto desarrollar en detalle la LOPD siendo de particular interés para el entorno de la Nube el Título VI que regula las transferencias internacionales de datos y el Título VIII en el que detalla las medidas de seguridad a aplicar a los ficheros que contengan datos de carácter personal. Las medidas de protección que deben ser aplicadas se establecen en función de la criticidad (a criterio del legislador) de los datos, y del impacto de su difusión en la protección de la persona. Se definen 3 niveles: Alto para datos muy cercanos a aspectos íntimos y definitorios de la persona; Medio para datos de tipo económico-social, y Bajo para el resto. Las medidas de protección aparecen descritas y detalladas y se definen dos de particular interés: responsabilidades sobre los ficheros, y ubicación geográfica de los mismos.
Observaciones	El Título VIII establece de forma detallada medidas de seguridad técnicas y organizativas a aplicar a los ficheros en función del tipo de datos tratados, estableciendo tres niveles incrementales de seguridad. El Reglamento define el concepto “transferencia internacional de datos”, cuando en una operación, datos de carácter personal van a cambiar su ubicación a otra fuera del ámbito legal de LOPD y su reglamento. En este caso, define las condiciones en las que se pueden mover que son: • Movimiento permitido si el destino es un país con un nivel de protección equivalente a España (países UE, y algunos más). • Movimiento requiere autorización administrativa para movimiento a otros países (EEUU incluido desde sentencia sobre Safe Harbour). El reglamento define los roles de: • Responsable del fichero, que corresponde con la entidad que ha recopilado los datos personales y pretende tratarlos (en entorno en la Nube corresponde con la empresa clinte); • y de Encargado del Tratamiento, que es la entidad que opera con los datos y los SS.II. Que los maneja (en un entorno en la Nube es el CSP) • Y exige la existencia de un contrato entre el Responsable del Fichero y el Encargado del Tratamiento, con contenidos mínimos sobre el mismo (Art. 12 LOPD).

ISO 27001

Nombre	Information technology - Security techniques - Information security management systems - Requirements	**Extensión del documento**	34
Versión en vigor	ISO IS 27001:2013	**Gratuito**	No
Organización que lo mantiene	International Organization for Standarization	**Año de aprobación**	2013

Objetivo	El estándar ISO27001 es la norma de certificación sobre el SGSI (Sistema de Gestión de Seguridad de la Información). Especifica los requisitos para establecer, implementar, mantener y mejorar de forma continua de un sistema de gestión de la seguridad de la información en una organización. También incluye los requisitos para el análisis, evaluación y tratamiento de los riesgos relacionados con la seguridad de la información, en base a las necesidades de la organización. Los requisitos que establece son genéricos y aplicables a todas las organizaciones, independientemente de su tipo, tamaño o naturaleza.
Observaciones	Es una norma certificable, por la que una empresa puede obtener una certificación oficial, pero en ninguna parte de la norma hace referencia explícita a servicios en la Nube. Sin embargo, puede ser aplicado por un CSP como referencia para implantar un proceso de mejora continua en seguridad en su entorno en la Nube, que conduzca a la mejora efectiva en este entorno. Este estándar se basa en solicitar que la empresa tenga en cuenta la disponibilidad, integridad y confidencialidad de la información. Es voluntario para las empresas, pero actualmente, el tenerlo es necesario si se quiere tener posibilidad de optar a ciertos concursos o proyectos. La versión actual es del 2013, influenciada por el Anexo A, donde la estructura del articulado de las normas actuales es si no parecido, idéntico, para poder tener un sistema de gestión corporativo y con los mismos componentes básicos (política, análisis de riesgos, ...).

ISO 20000-1

Nombre	Information technology - Service management - Part 1: Service management system requirements		**Extensión del documento**	38
Versión en vigor	ISO IS 20000-1:2011		**Gratuito**	No
Organización que lo mantiene	International Organization for Standarization		**Año de aprobación**	2011

Objetivo	Esta norma recoge los requisitos que se deben incluir en el diseño, transición, provisión y la mejora de los servicios TIC para cumplir con los requerimientos de los mismos, y aportar valor tanto para el cliente como para el propio proveedor del servicio. La norma requiere del proveedor un enfoque basado en procesos integrados a la hora de planificar, establecer, implementar, operar, controlar, revisar, mantener y mejorar un Sistema de Gestión del Servicio.
Observaciones	Esta norma establece los requerimientos para implementar un Sistema de Gestión del Servicio, coherente con el esquema establecido por ISO para los distintos sistemas de gestión (ISO 9001, ISO 14001, ISO 27001, etc.). Aunque no se trata de una norma específica para proveedores de servicios en la Nube, establece los requerimientos que debe tener en cuenta cualquier proveedor a la hora de gestionar el ciclo de vida completo de la prestación de un servicio. En este sentido no tiene capítulos o secciones de servicios en la Nube, sino que establece los requerimientos que debe cumplir una organización a la hora de establecer los procesos para el diseño de los servicios, la provisión de los mismos, la relación con terceros, la resolución de incidencias y problemas, y finalmente los procesos de control de dichos servicios. La norma tiene dos partes. La ISO 20000-1 establece los requerimientos del Sistema de Gestión del Servicio. La ISO 20000-2 es un documento más amplio que constituye una guía para ayudar a interpretar los requerimientos de la ISO 20000-1 de forma más precisa, permitiendo por lo tanto utilizarla de una manera más efectiva.

CSA-OCF

Nombre	Cloud Security Alliance Open Certification Framework	**Extensión del documento**	8
Versión en vigor	1	**Gratuito**	Si
Organización que lo mantiene	Cloud Security Alliance	**Año de aprobación**	2012

Objetivo	Permitir una certificación global, acreditada y basada en la confianza para proveedores de servicios en la Nube.
Observaciones	Define un modelo basado en la implantación de elementos de Gobierno del Modelo, de los Servicios prestados en la Nube, de la Organización, de Gestión del Riesgo y de Auditoría de los elementos. Más que un esquema de certificación, es un modelo que soporta varios esquemas de certificación y permite modular el nivel de exigencia y rigor aplicable a por un CSP a sus distintos servicios en la Nube y les permite evolucionar y madurar a lo largo del tiempo. Establece tres niveles de exigencia en la acreditación: 1. Cuestionario de autoevaluación, que se comunica a CSA para su publicación. 2. Certificación acreditada por una entidad independiente. 3. Modelo continuo de monitorización, auditoría y seguimiento de seguridad en la prestación de servicio.

CSA-STAR

Nombre	Cloud Security Alliance Security, Trust & Assurance Registry	**Extensión del documento**	171 (csa-guide)
Versión en vigor	2013	**Gratuito**	No
Organización que lo mantiene	Cloud Security Alliance	**Año de aprobación**	2013

Objetivo	Establece un modelo de certificación de Proveedores de Servicios en la Nube promovido por CSA. Corresponde con el segundo nivel de certificación (certificación acreditada por una entidad independiente), en el marco del modelo Open Certification Framework (OCF).
Observaciones	Es una certificación que requiere ser emitida por una entidad de certificación autorizada y controlada por un esquema de acreditación. De esta forma, la certificación ofrece garantías a los usuarios de los servicios de la entidad certificada. Todos estos elementos conforman un escenario de confianza para el consumidor de servicios en la Nube, disponiendo de criterios de comparación objetivos entre CSP en los que soportar la selección de los mismos. Se apoya en la Guía de Controles de Seguridad para Entornos en la Nube, de CSA (CSA-Guide), y en su Matriz de Controles para la Nube (CCM), como biblioteca de controles de seguridad cuya implantación deben ser verificada.

ECSA

Nombre	EuroCloud Star Audit	**Extensión del documento**	N/A
Versión en vigor	2013	**Gratuito**	No
Organización que lo mantiene	EuroCloud	**Año de aprobación**	2013

Objetivo	Es un modelo de Certificación de CSP promovido por Eurocloud, enfocado en la certificación de los servicios en la Nube prestados por los CSPs, en tanto que cumplen con los requisitos contractuales, técnicos y organizativos que la organización ha definido para dichos servicios.
Observaciones	La certificación es emitida por auditores cualificados por Eurocloud, de acuerdo a los requisitos establecidos en cada momento por la propia organización. La obtención de esta certificación requiere del CSP transparencia en la forma en la que presta sus servicios, incluyendo la ubicación de la información que gestiona y donde se procesa, información del CSP y su catálogo de servicios, así como del ciclo de vida de los mismos (cambios, evoluciones, corrección, integridad de los mismos). La certificación requiere también la inspección in situ por el equipo auditor del CSP y sus instalaciones.

PCI DSS

Nombre	Payment Card Industry Data Security Standard	**Extensión del documento**	115
Versión en vigor	3.1	**Gratuito**	Si
Organización que lo mantiene	Payment Card Industry (PCI) Security Standard Council	**Año de aprobación**	2015

Objetivo	PCI se trata de una normativa de cumplimiento obligatorio para poder gestionar, tramitar y/o almacenar datos de tarjeta de crédito, bien sea el PAN (Personal Account Number o número de tarjeta) o cualquier otro dato identificativo de una tarjeta. Cada entidad (VISA, MasterCard, American Express, ...) pone unas condiciones algo especiales, pero esta normativa está aceptada como base por todas y cada una de las grandes firmas de tarjetas de pago.
Observaciones	No existen, en esta norma, referencias específicas a aspectos relacionados con la computación en la Nube. Ante las insistencias de este entorno creciente, el Council de PCI sacó unas recomendaciones (Guidelines) en un documento PDF. En este documento queda claro, de los diferentes requerimientos que hay cumplir de la norma, los que tienen responsabilidad por parte exclusiva del CSP, los de cliente y los que ambos tienen acciones a tomar, tanto para entornos IaaS, PaaS y SaaS; también comenta el apartado de SecaaS.

SSAE 16

Nombre	Statement on Standards for Attestation Engagements No. 16	**Extensión del documento**	Variable
Versión en vigor	SSAE 16 - AT 801	**Gratuito**	No
Organización que lo mantiene	American Institute of Certified Public Accountants (AICPA)	**Año de aprobación**	2011

Objetivo	Es una norma de análisis y evaluación (no de auditoría) para la realización de verificaciones independientes del cumplimiento de los controles y de la eficacia de éstos, con el objetivo de obtener unos informes que evidencien que los controles internos de una organización que presta servicios a terceros son adecuados. Las verificaciones se centran principalmente en los controles que puedan afectar a los estados financieros de los clientes de la organización evaluada.
Observaciones	Es el estándar de referencia para revisar a las organizaciones prestadoras de servicios, y sustituye al estándar SAS 70. Está ampliamente extendido en EEUU, si bien está alineado con el estándar ISAE 3402. La verificación es llevada a cabo por un auditor externo, quién presenta una opinión sobre los controles de la organización en base a si la descripción de los mismos es adecuada, si se han diseñado eficazmente, si se han puesto en marcha en una fecha especifica, y si se ejecutan con eficacia durante un periodo de tiempo. Se expresa por medio de un informe SOC (Service Organization Control, existiendo SOC 1, SOC 2 y SOC 3) el cual a su vez puede ser de Tipo I si recoge la descripción del sistema y la idoneidad del diseño de los controles, o de Tipo II si además incluye una descripción detallada de las pruebas realizadas sobre los controles de la organización durante un periodo mínimo de seis meses. No incluye un conjunto específico de controles de seguridad, ni específicos de la Nube, si bien se suelen utilizarse por parte de proveedores de servicios para medir y mostrar a sus clientes, la seguridad: disponibilidad, confidencialidad e integridad. En este tipo de servicios, la certificación en SSAE 16 puede resultar interesante, ya que mediante los informes de auditoría generados a tal efecto se consigue un análisis de la seguridad de la información de, sus niveles de disponibilidad, confidencialidad y privacidad, y demás aspectos que resultan fundamentales a la hora de almacenar datos en la nube.

CSA CCSK

Nombre	Cloud Security Alliance Certificate of Cloud Computing Knowledge	**Extensión del documento**	167-CSAguide
Versión en vigor	V3	**Gratuito**	No
Organización que lo mantiene	Cloud Security Alliance	**Año de aprobación**	V1-2010 V3-2013

Objetivo	Evalúa el conocimiento del profesional sobre los escenarios y requisitos de seguridad específicos de los entornos en la Nube. Los entornos en la Nube tienen características específicas, derivadas de la forma en la que se prestan sus servicios, las tipologías y ubicación de sus usuarios y la base tecnológica de los servicios en la Nube. Estas características hacen surgir nuevos requisitos (efectos Locked-In, multitenancy, etc), que requieren de nuevos controles de seguridad, específicos para este entorno.
Observaciones	Acredita el conocimiento y capacidad del candidato para aplicar los controles seguridad de la Guía de Controles de Seguridad para Entornos en la Nube (CSA-Guide) de la forma más efectiva. La acreditación cubre los siguientes campos: • Arquitecturas en la Nube • Riesgo Corporativo. Gobierno. • Requisitos legales y e-Discovery. • Cumplimiento Legal y Auditoría • Gestión del Ciclo de Vida de la Información. • Portabilidad. Interoperabilidad. • Seguridad clásica, Continuidad de Negocio y Recuperación ante Desastres • Operaciones en el Centro de Datos • Respuesta a Incidentes. • Seguridad de Aplicaciones • Cifrado y Gestión de Claves • Gestión de Identidades y de Accesos. • Virtualización • SecaaS (Security-as-a-Service) La certificación CCSK está disponible en español y en inglés.

CSA CCSP

Nombre	Cloud Security Alliance Certified of Cloud Security Professional	**Extensión del documento**	N/A
Versión en vigor	2015	**Gratuito**	No
Organización que lo mantiene	Cloud Security Alliance e ISC^2	**Año de aprobación**	2015

Objetivo	Respaldar los conocimientos y experiencia de los profesionales que trabajan en entornos en la Nube, con un enfoque no solo técnico, sino de negocio para aprovechar las oportunidades de mejora de las organizaciones que ofrecen servicios en la Nube.
Observaciones	La certificación CCSP es pues interesante tanto para los profesionales que trabajan en proveedores de servicios en la Nube, como en organizaciones que consumen estos servicios, pudiendo mejorar en ambos casos mediante el adecuado y seguro uso de la Nube. CCSP desarrolla su cuerpo de conocimiento en las siguientes seis (6) áreas: • Architectural Concepts & Design Requirements • Cloud Data Security • Cloud Platform & Infrastructure Security • Cloud Application Security • Operations • Legal & Compliance

ISO 27002

Nombre	Information technology - Security techniques - Code of practice for information security controls	**Extensión del documento**	94
Versión en vigor	ISO IS 27002:2013	**Gratuito**	No
Organización que lo mantiene	International Organization for Standarization	**Año de aprobación**	2013

Objetivo	Proporcionar una referencia para la selección de controles para la gestión de la seguridad de la información. Se puede utilizar como referencia para la selección de los controles en el proceso de implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO / IEC 27001, o como una guía para las organizaciones que quieran implantar controles comúnmente aceptados para gestionar la seguridad de seguridad de la información. También se puede utilizar esta norma en el desarrollo de directrices de gestión de seguridad de la información, teniendo en cuenta sus riesgos específicos para la seguridad de información.
Observaciones	Es una parte no certificable, pero que indica las preguntas en base al Anexo A de la norma ISO27001 que deben hacerse para implantar un sistema de gestión adecuado. En esta recolección de buenas prácticas, hace referencia a los servicios en la Nube, básicamente en el apartado 15.1.3, donde hace referencia a los contratos con los proveedores, especificando que los proveedores de servicios en la Nube deben tenerse en cuenta en este apartado. También están disponibles controles de seguridad, genéricos para cualquier escenario, por lo que también contribuyen a mejorar la seguridad de la Nube.

ISO 27018

Nombre	Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors	**Extensión del documento**	23
Versión en vigor	ISO IS 27018:2014	**Gratuito**	No
Organización que lo mantiene	International Organization for Standarization	**Año de aprobación**	2014

Objetivo	Establece los objetivos de control, controles y directrices comúnmente aceptados para implementar medidas de protección de información de identificación personal (PII) de acuerdo con los principios de privacidad establecidos por la norma ISO / IEC 29100 para entornos de Nube Pública. Establece directrices basadas en la norma ISO / IEC 27002, teniendo en cuenta los requisitos normativos para la protección de PII que podría ser aplicable en el contexto de la gestión de riesgos de seguridad de la información de un proveedor de servicios de Nube Pública.
Observaciones	Se trata de un código de buenas prácticas basado en los objetivos de control y controles establecidos en la norma ISO 27002:2013. Para cada uno de los controles, indica si aplica tal cual está redactado en la ISO 27002, y en los casos en los que procede añade para dicho control guías de implantación e información adicionales, orientadas específicamente a la protección de información de identificación personal en entornos de Nube Pública. Además de los objetivos de control y controles incluidos en la ISO 27002, incorpora en su anexo A otros 11 objetivos de control, que incluyen 25 controles adicionales específicos para la protección de información de identificación personal en entornos de Nube Pública.

CSA CCM

Nombre	Cloud Security Alliance Cloud Control Matrix	**Extensión del documento**	Excel
Versión en vigor	v3.0.1	**Gratuito**	Sí
Organización que lo mantiene	Cloud Security Alliance	**Año de aprobación**	2014

Objetivo	Proporcionar los principios fundamentales de seguridad para los proveedores de Nube y para ayudar a los clientes a valorar el riesgo de seguridad de un proveedor. Está diferenciado en función del modelo de Nube y el entorno y proporciona un marco en 16 dominios que se contrastan con otros estándares aceptados en la industria, regulaciones y otros marcos de control, todo ello para reducir la complejidad de una auditoría. Persigue normalizar las expectativas de seguridad, la taxonomía de la Nube, la terminología y las medidas de seguridad a implementar.
Observaciones	El CCM v3.0.1 tiene 133 controles estructurados en 16 dominios y se proporciona en formato Microsoft Excel. Cada control se mapea con las regulaciones, normas, estándares y guías principales de aplicación en el entorno de la Nube. El capítulo español de CSA traduce periódicamente el CCM al español y mapea sus controles con el Reglamento de la LOPD y el Esquema Nacional de Seguridad.

CIF COP

Nombre	Cloud Industry Forum Code of Practice	**Extensión del documento**	14, 15, 23, 5 y 7
Versión en vigor	NA	**Gratuito**	0
Organización que lo mantiene	Cloud Industry Forum	**Año de aprobación**	NA

Objetivo	El propósito de este referencial es lograr una mayor transparencia y confianza para hacer negocios en en la Nube. Los proveedores certificados declaran y se comprometen a prestar un servicio de calidad, de acuerdo con las directrices y buenas prácticas establecidas en el CIF COP. Es un marco integral que permite a los proveedores de servicios contrastar la forma de la que opera, con las normas elaboradas por la industria para la prestación de servicios en la Nube. Se centra en la transparencia, la responsabilidad y las competencias para operar en la Nube.
Observaciones	Se trata de un esquema de certificación con varios documentos. El Documento 1 es un resumen ejecutivo del esquema, el 2 establece cómo realizar una certificación de primera parte, el 3 es una guía para proveedores de servicios en la Nube. Además incluye un documento de código de buenas prácticas y otro de términos y condiciones. El referencial especifica el ciclo de vida completo de la certificación a través de las siguientes fases: Identificar la necesidad, determinar los requerimientos, solicitar el registro, preparar, analizar, corregir, declarar, validar, autorizar y publicar. Los requerimientos están distribuidos en los apartados de transparencia, responsabilidad y competencias. Con respecto a las medidas de seguridad, pide conformidad con “Consensus Assessments Initiative Questionnaire from the Cloud Security Alliance”. También contempla dentro del cuestionario de autoevaluación el que la organización tenga otros sistemas de gestión certificados (ISO 9001, 14001, 27001, etc.), así como las asociaciones sectoriales de relevancia en las que participa.

CCN STIC 823

Nombre	Guía de seguridad de las TIC - Utilización de servicios en la nube	**Extensión del documento**	45
Versión en vigor	41974	**Gratuito**	Si
Organización que lo mantiene	Gobierno de España, Ministerio de la Presidencia, Centro Nacional de Inteligencia, Centro Criptológico Nacional	**Año de aprobación**	2014

Objetivo	Recoge los aspectos de seguridad necesarios que deberán contemplarse para la adopción de la Nube como paradigma tecnológico para la disposición de servicios con las garantías de seguridad pertinentes. Identifica las medidas de seguridad y los requisitos que deben cumplir los proveedores de servicios en la Nube para dar cumplimiento tanto a los marcos legislativos aplicables, en especial el Esquema Nacional de Seguridad o la normativa vigente en materia de protección de datos personales, como a los códigos de buenas prácticas o estándares reconocidos internacionalmente.
Observaciones	Incluye una descripción de los distintos modelos de Nube, así como de los servicios asociados a los mismos y sus características. Como referencia principal para identificar las medidas a tener en cuenta sigue los aspectos que son de aplicación en el ENS, es decir, gestión de riesgos, la gestión de servicios externo, la categorización según el Anexo I del ENS, el cumplimiento de las medidas del ANEXO II del ENS que sean de aplicación y otros requisitos legales como los provenientes de la LOPD. Igualmente detalla las medidas a adoptar en el marco de los procesos de contratación, operación, supervisión y auditoría.

Article 29 WP 196

Nombre	Opinion 05/2012 on Cloud Computing del Article 29 data protection working party	**Extensión del documento**	27
Versión en vigor	01037/12/EN	**Gratuito**	Si
Organización que lo mantiene	Article 29 data protection working party (conjunto de las Agencias de Protección de Datos europeas)	**Año de aprobación**	2012

Objetivo	Analizar todos los aspectos relevantes para los proveedores de servicios en la Nube que operan en el Área Económica Europea y a sus clientes, especificando todos los principios aplicables de la Directiva Europea de Protección de Datos (95/46/EC) y la Directiva de e-privacidad 2002/58/EC (revisada en 2009/136/EC) donde sean relevantes.
Observaciones	La Opinión analiza los riesgos de la Nube desde el punto de vista de la protección de datos, revisa en detalle el marco legal aplicable y establece una serie de conclusiones y recomendaciones para proveedores y clientes. Como conclusión se enfatiza la importancia de que los clientes hagan un análisis de riesgos y de que los proveedores proporcionen la información suficiente para ello, así como la importancia de cumplir el marco legal. El establecimiento de una apropiada regulación contractual es muy importante así como verificar que se cumple la regulación en materia de transferencias internacionales de datos. Se ve como positivo el uso de certificaciones de terceros respecto a la protección de datos personales. Las recomendaciones del Grupo del Artículo 29 se han tomado como base para el Reglamento Europeo de Protección de Datos, si bien el porcentaje de adopción de las mismas en el reglamento no será conocido hasta la publicación efectiva del reglamento.

Guía APD Clientes Cloud

Nombre	Guía para clientes que contraten servicios de Cloud Computing	**Extensión del documento**	24
Versión en vigor	0	**Gratuito**	Si
Organización que lo mantiene	Gobierno de España, Ministerio de Justicia, Agencia Española de Protección de Datos	**Año de aprobación**	2013

Objetivo	Proporcionar un conocimiento básico de la Nube a sus clientes para a continuación explicar las garantías contractuales, riesgos, estrategia a seguir, conocimientos básicos de protección de datos y un apartado específico para administraciones públicas.
Observaciones	Es un documento de carácter divulgativo y didáctico que puede servir de introducción y facilitar la comprensión de la regulación de protección de datos en la Nube desde el punto de vista del cliente.

Guía APD Proveedores Cloud

Nombre	Orientaciones para prestadores de servicios de Cloud Computing	**Extensión del documento**	10
Versión en vigor	0	**Gratuito**	Si
Organización que lo mantiene	Gobierno de España, Ministerio de Justicia, Agencia Española de Protección de Datos	**Año de aprobación**	2013

Objetivo	Complementar a la Guía para clientes de servicios en la Nube proporcionando orientaciones a los proveedores de servicios en la Nube.
Observaciones	Este documento es complementario de la Guía para clientes a la cual hace referencia. Trata aspectos específicos para los proveedores tales como los relativos a la contratación, transferencias internacionales de datos, ejercicio de derechos y contratación con las administraciones públicas

Anexos

Marcos que se tendrán en cuenta en próximas versiones

El capítulo español de Cloud Security Alliance (CSA-ES) tiene previsto darle continuidad a este estudio, de forma que en siguientes versiones se pretende incluir en el mismo al menos los siguientes marcos de referencia:

- Legislación aplicable
  - Ley de Administración Electrónica
  - Futuro Reglamento Europeo de Protección de Datos
- Certificaciones de sistema
  - Leet Security
  - European Privacy Seal (EuroPriSe)
  - Federal Risk and Authorization Management Program (FedRAMP)
- Certificaciones profesionales
  - Amazon Web Services Certified Solutions Architect (AWS – CSA)- Professional
  - Rackspace Cloud U
  - IBM Certified Solution Advisor – Cloud Computing Architecture (IBM CSA-CCA)
  - IBM Certified Solution Architect - Cloud Computing Infrastructure (IBM CSA-CCI)
  - IBM Certified Application Developer – Cloud Platform (IBM CAD-CP)
  - Google Certified Deployment Specialist
  - Red Hat Certified Architect: Cloud
  - Cloud School Certified Cloud Technology Professional (CCTP)
  - Microsoft Certified Solutions Expert (MCSE): Private Cloud
  - VMWare Certified Professional 6 (VCP6) – Cloud
- Códigos de buenas practicas
  - NIST SP 800-146 Cloud Computing Synopsis and Recommendations
  - ISACA COBIT 5
- Guías de uso
  - NIST SP 500-307 Cloud Computing Service Metrics Description

Términos y definiciones empleados en el análisis de Marcos de Referencia

Los siguientes términos y definiciones son aplicables para los propósitos del presente informe.

- **Ámbito España:** Marco de referencia cuya aplicación sólo es relevante en España
- **Ámbito nacional otros países:** Marco de referencia cuya aplicación sólo es relevante en un único país (por ejemplo EEUU, Francia, Reino Unido, etc.) distinto a España
- **Ámbito europeo:** Marco de referencia que es aplicable a todos los países pertenecientes a la Unión Europea
- **Ámbito internacional:** Marco de referencia que es aplicable en cualquier país.
- **Certificación de primera parte**: Certificaciones emitidas por la propia empresa que va a ostentar el certificado
- **Certificación de segunda parte**: Certificaciones emitidas por una segunda empresa, distinta a la que va a ostentar el certificado
- **Certificación de tercera parte**: Certificaciones emitidas por una institución independiente de las partes interesadas, acreditada y reconocida para emitir el certificado, como órgano independiente, confiable y habilitado por las partes involucradas
- **Código de buenas prácticas**: Documento que recoge un conjunto de métodos o técnicas que han demostrado de forma consistente mejores resultados que los obtenidos empleando otros medios. Se utiliza como marco de referencia o de evaluación.
- **CSP:** Proveedor de servicios en la Nube, de sus siglas en Ingles Cloud Service Provider.
- **Cuerpo de conocimiento**: (del Inglés Body of Knowledge) es un conjunto completo de conceptos, términos y actividades que conforman un ámbito profesional, tal como lo establece una entidad, organismo o asociación profesional relevante.
- **Específico producto**: Hace referencia a productos hardware o software específicos
- **Específico servicio**: Hace referencia a servicios específicos (Cloud Storage, Cloud Hosting, Software as a Service, etc.)
- **Específico tecnología**: Hace referencia a tecnologías específicas (almacenamiento, SDN, procesamiento, prevención de intrusiones, etc.).
- **Gobierno IT**: El conjunto de procesos que aseguran el uso eficaz y eficiente de IT para conseguir que una organización logre sus objetivos.
- **Norma**: Es un documento establecido por consenso y aprobado por un organismo internacional reconocido, que proporciona reglas, directrices o características para actividades o sus resultados, con la finalidad de alcanzar un nivel óptimo de organización en un determinado contexto.
- **Orientación a profesionales:** Marco de referencia orientado a personas y profesionales individuales.
- **Orientación a sistemas TIC:** Marco de referencia orientado a Marco de referencia orientado a su aplicación en sistemas de información.
- **Orientación a procesos y procedimientos:** Marco de referencia orientado a los procesos y procedimientos de una organización.
- **Orientación a Gobierno IT:** Marco de referencia orientado al gobierno IT de la organización

Bibliografía

1. Certification in the EU Cloud Strategy, ENISA: resilience.enisa.europa.eu/cloud-computing-certification/certification-in-the-eu-cloud-strategy
2. Cloud Certification Schemes Metaframework, ENISA: www.enisa.europa.eu/media/press-releases/enisa-cloud-certification-schemes-metaframework
3. Esquema Nacional de Seguridad: www.boe.es/diario_boe/txt.php?id=BOE-A-2010-1330
4. Esquema Nacional de Interoperabilidad: www.boe.es/diario_boe/txt.php?id=BOE-A-2010-1331
5. Ley organica de protección de datos de carácter personal: www.boe.es/buscar/act.php?id=BOE-A-1999-23750
6. Reglamento de desarrollo de la ley organica de protección de datos de carácter personal: www.boe.es/buscar/act.php?id=BOE-A-2008-979
7. Cloud Industry Forum Code of Practice: cloudindustryforum.org/code-of-practice/code-of-practice
8. Article 29 Working Party 196: ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf
9. Guía APD Clientes Cloud: www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_Cloud.pdf
10. Guía APD Proveedores Cloud: https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/ORIENTACIONES_Cloud.pdf
11. Guía CCN STIC 823: www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/823-Seguridad-en-entornos-cloud/823-Cloud_Computing_ENS.pdf
12. PCI-DSS: www.pcisecuritystandards.org/pdfs/PCI_DSS_v2_Cloud_Guidelines.pdf
13. CSA-OCF : cloudsecurityalliance.org/group/open-certification/
14. CSA-STAR : cloudsecurityalliance.org/star/certification/
15. ECSA : eurocloud-staraudit.eu/
16. CCSK: cloudsecurityalliance.org/education/ccsk/
17. CCSP: www.isc2.org/ccsp/default.aspx
18.

CSA ES cloud security SPAIN alliance SM

isms forum spain

Paseo de la Habana, 54,
2º Izquierda 1.
28036 Madrid - España
Tlf :+34 91 563 50 62

+info:
info@ismsforum.es
www.ismsforum.es
@ISMSForumSpain