Seguridad y resistencia en las nubes de la Administración Pública

Informe para la toma de decisiones

Enero 2011

enisa
European Network and Information Security Agency

Sobre ENISA

La Agencia Europea de Seguridad de las Redes y de la Información (ENISA) es una agencia de la UE creada para potenciar el funcionamiento del mercado interior. ENISA es un centro de conocimiento especializado para los Estados miembros europeos e instituciones europeas en materia de seguridad de las redes y de la información. Ofrece asesoramiento y recomendaciones, y sirve como central de información y comunicación para el ejercicio de buenas prácticas. Además, la agencia facilita el contacto entre las instituciones europeas, los Estados miembros y las actividades de negocio privadas y los agentes del sector.

Esta obra tiene lugar en el contexto del programa Emerging and Future Risks (Riesgos emergentes y futuros) de ENISA.

La redacción del presente informe corresponde a D. Daniele Catteddu.

La traducción al español del informe es una cortesía del Instituto Nacional de Tecnologías de la Comunicación, INTECO www.inteco.es . España.

Datos de contacto:

Daniele.catteddu@enisa.europa.eu

Internet: http://www.enisa.europa.eu/

Aviso legal
Se advierte de que esta publicación representa las opiniones e interpretaciones de los autores y redactores, salvo que se indique otra cosa. La presente publicación no deberá interpretarse como una actuación de ENISA o de los organismos de ésta, salvo que se adoptase en virtud del Reglamento (CE) n°. 460/2004 de ENISA. Esta publicación no incluye necesariamente los conocimientos más avanzados, y es posible que se hagan actualizaciones de la misma en el futuro.
Las fuentes tomadas de terceros aparecen citadas como corresponde. ENISA no se hace responsable del contenido de las fuentes externas, lo que incluye los sitios web externos a los que se hace referencia en esta publicación.
El propósito de esta publicación se limita exclusivamente a fines educativos e informativos. Ni ENISA ni ninguna otra persona que actúe en nombre de ésta se hará responsable del uso que pueda hacerse de la información que se incluye en esta publicación.
Se autoriza la reproducción, siempre que se cite la fuente.
© European Network and Information Security Agency [Agencia Europea de Seguridad de las Redes y de la Información] (ENISA), 2010

Lista de colaboradores

La elaboración de la presente obra corresponde a un redactor de ENISA, que ha contado con la participación y comentarios de un grupo seleccionado por sus conocimientos especializados sobre la materia y que incluye expertos del sector, del mundo académico y de las administraciones públicas.

Las opiniones que se expresan en la presente publicación corresponden a su redactor, salvo que se indique otra cosa, y no reflejan necesariamente las opiniones de los expertos que participan en ella.

Miembros del grupo de expertos por orden alfabético:

Amanda Goodger, CESG, Reino Unido.

Andrea Glorioso, Comisión Europea (observadora).

Prof. Antonio Lioy, Politecnico di Torino, Italia.

Ben Katsumi, IPA, Japón.

Daniele Catteddu, ENISA (presidencia).

David Wright, Trilateral Research & Consulting LLP, Reino Unido.

Dennis Heinson, LL.M. (UCLA), Universität Kassel (provet)/Center of Advanced Security Research [Centro de Investigación Avanzada sobre Seguridad] Darmstadt (CASED), Alemania.

Dr. Giles Hogben, ENISA.

Prof. Fabrizio Baiardi, Dipartimento di Informatica, Università di Pisa, Italia.

Jim Reavis, Cloud Security Alliance, Estados Unidos.

Liam Lynch, eBay, Estados Unidos.

Marcos Gómez, INTECO, Instituto Nacional de Tecnologías de la Comunicación, España.

Prof. Dr. Milan Petkovic, Philips Research Eindhoven y Universidad Técnica de Eindhoven, Países Bajos.

Dr. Paolo Balboni, Balboni Law Firm, Tilburg University, European Privacy Association, Italia.

Dr. Peter Dickman, Google, Suiza.

Philippe Massonet, CETIC – Proyecto RESERVOIR, Bélgica.

Raj Samani, McAfee, EMEA

Rui Barros, ELANET (Red Telemática de Autoridades Locales Europeas) (CEMR) - European Network for eGovernment and Information Society (Red Europea de Administración Electrónica y Sociedad de la Información) (con el respaldo del Consejo Europeo de Municipios y Regiones).

Dr. Srijith Nair, British Telecom, Reino Unido.

Dr. Theo Dimitrakos, British Telecom, Reino Unido.

Steffen Schreiner, CASED, Alemania / CERN, Suiza.

Índice

Sobre ENISA 2
Datos de contacto: 2
Índice 4
Resumen 7
Recomendaciones a las administraciones públicas y a los organismos públicos 9
1. Introducción 12
1.1. Estructura del informe y guía de lectura 13
1.2. Situación hipotética introductoria: Tomar una decisión 15
2. Objetivos y análisis 23
2.1. Destinatarios 24
2.2. Método de análisis 24
3. Modelo para responsables de la toma de decisiones 26
3.1. Parámetros de seguridad y resistencia 29
Servicio de extremo a extremo seguro y fiable 30
Parámetros de selección de seguridad y resistencia 31
3.2. Variables de negocio y operativas 38
Tipos de datos 38
Perfil de usuario 38
Escalabilidad y gestión de capacidad 39
Interoperabilidad de interfaz 39
Colaboración 39
Costo y presupuesto 40
Propiedad 40
3.3. Marco legal y regulador 40
Consideraciones legales generales 40

Soberanía y control gubernamentales sobre la información y los datos: cuestiones sobre el acceso a la aplicación de la ley, la confidencialidad y la propiedad intelectual 41
Contratación pública 41
Protección de datos y seguridad de los datos 41
Disposiciones sobre Interoperabilidad / Transferencias al origen / "Cautividad del mercado" 45
Negligencia profesional del proveedor de servicios en la nube 45
La subcontratación de servicios en la nube y el cambio de control del proveedor de servicios en la nube 46
3.4. Opciones de arquitectura 46
No nube 46
Nube 47
4. Análisis DAFO 49
4.1 Nube pública 50
Puntos fuertes 50
Puntos débiles 51
Oportunidades 52
Amenazas 53
4.2. Nube privada 54
Puntos fuertes 54
Puntos débiles 55
Oportunidades 55
Amenazas 56
4.3. Nube comunitaria 57
Puntos fuertes 57
Puntos débiles 57
Oportunidades 58
Amenazas 58

5. Situaciones hipotéticas que sirven como ejemplo 59
5.1 Descripción del servicio 59
5.2. Parámetros y requisitos 62
5.3. Evaluación comparativa de riesgos 67
5.4. Selección de la solución e identificación de amenazas y debilidades 75
6. Preparación de una solicitud de oferta 77
7. Conclusiones y recomendaciones 81
7.1 Recomendaciones a gobiernos, administraciones y organismos públicos 83
8. Glosario 87
9. Referencias 92
Anexo I – Análisis jurídico 94
Anexo II – Situaciones hipotéticas 116
Situación hipotética de atención sanitaria – situación núm. 1 116
Historia clínica electrónica (HCE) 118
Archivos electrónicos sanitarios 120
Sistema regional de intermediación e intercambio de registros electrónicos de pacientes 120
Nube comunitaria local y regional – situación núm. 2 120
Procedimientos administrativos electrónicos 125
Nube gubernamental como vivero de empresas - situación hipotética núm. 3 126
Modelo J-SaaS 127
Anexo III - Descripción de la arquitectura del Proyecto Reservoir 129
Arquitectura de nube virtual para nubes comunitarias 129
Amenazas de extremo a extremo a la resistencia de una arquitectura de nube virtualizada 130
Amenazas a la resistencia de extremo a extremo en nubes comunitarias 132
Anexo IV – Lista de amenazas 134

Resumen

La computación en la nube ofrece una gran cantidad de beneficios potenciales a los organismos públicos, como la escalabilidad, la elasticidad, el alto rendimiento, la resistencia y la seguridad, además de la rentabilidad de costes. Comprender y gestionar los riesgos relacionados con la adopción e integración de las prestaciones de la computación en la nube en los organismos públicos supone un reto clave. La gestión eficaz de las cuestiones sobre seguridad y resistencia en relación con las prestaciones de la computación en la nube está llevando a muchos organismos públicos a innovar y, en ciertos casos, a replantearse sus procesos de evaluación del riesgo y de toma de decisiones fundadas respecto a este nuevo modelo de prestación de servicios.

En este informe se identifica un modelo de toma de decisiones del que podrán valerse los responsables de dirección a la hora de decidir de qué modo pueden llevar los requisitos operativos, jurídicos y de seguridad de la información a la identificación de la solución de arquitectura de computación que mejor se adapte a las necesidades de su organización. Los objetivos principales del informe son:

- Poner de relieve las ventajas e inconvenientes, en cuanto a la seguridad de la información y la resistencia, de los modelos de computación en la nube comunitarios, privados y públicos.
- Guiar a los organismos públicos en la definición de sus requisitos de seguridad de la información y resistencia al evaluar los modelos de prestación de servicios de la computación en la nube.

Además, este informe pretende brindar apoyo, de forma indirecta, a los Estados miembros de la Unión Europea en la definición de su estrategia nacional respecto a la nube en lo que a seguridad y resistencia se refiere.

La guía sobre toma de decisiones que se propone servirá de ayuda a los lectores a la hora de comparar los modelos de nube comunitarios, privados y públicos, y de decidir acerca del modelo de implementación del servicio de tecnologías de la información (TI) más adecuado, de los controles que deban aplicarse y de las cuestiones clave que deban solicitarse a un proveedor de servicios de cara a reducir los riesgos que supone la migración a la computación en la nube, a un nivel que resulte conforme con su tolerancia a los riesgos.

El análisis se basa en tres situaciones hipotéticas de uso de la computación en la nube: asistencia sanitaria, administración pública local e infraestructura de computación en la nube de titularidad pública como vivero de empresas, ya que hemos asumido que los citados casos prácticos de uso del modelo resultan particularmente interesantes para los Estados miembros de la UE.

La herramienta empleada en este informe para comparar las ventajas e inconvenientes de la seguridad y resistencia de los modelos de computación en la nube comunitarios, privados y públicos es un análisis DAFO (en inglés, SWOT: puntos fuertes, puntos débiles, oportunidades y amenazas), el cual, en el caso de la toma de decisiones fundadas basadas en riesgos, habrá de emplearse de forma conjunta

con la evaluación de la seguridad descrita en el informe de ENISA *Cloud Computing: benefits, risks and recommendations for information security*. Es conveniente que los organismos públicos realicen siempre un riguroso análisis de riesgos de sus aplicaciones específicas en el contexto del modelo de nube, y este informe deberá considerarse un documento y una guía de apoyo.

Hemos llegado a la conclusión, como resultado de nuestro análisis, de que el modelo de servicio de computación en la nube satisface la mayor parte de las necesidades de las administraciones públicas, por una parte, porque ofrece escalabilidad, elasticidad, alto rendimiento, resistencia y seguridad. No obstante, muchos organismos públicos no han creado aún un modelo de evaluación de los riesgos para su organización en relación con la seguridad y la resistencia. La gestión de la seguridad y la resistencia en entornos de TI tradicionales supone de por sí un gran reto para los organismos públicos. Y la computación en la nube presenta algunos desafíos más. Por ejemplo, comprender el cambio en el equilibrio entre la responsabilidad (*responsibility*) y la rendición de cuentas (*accountability*) en el caso de funciones clave tales como la gobernanza y el control sobre los datos y las operaciones de TI, garantizar el cumplimiento de la legislación y la normativa y, en ciertos casos, la baja calidad de las conexiones a Internet en ciertas zonas de la Unión Europea (1).

Al parecer, tal cambio hacia la gobernanza y el control indirectos sobre los datos e infraestructuras de la TI constituye un reto inherente a la migración al modelo de nube (sobre todo, en lo que concierne a las nubes de tipo público y distribuciones de SaaS (Software como Servicio)), incluso a pesar de que, tal como ya ha indicado ENISA (p. ej., en su informe de 2009), es posible mejorar la situación logrando transparencia en el mercado y negociando los términos contractuales adecuados.
Las legislaciones y normativas nacionales de los Estados miembros de la Unión Europea imponen en la actualidad restricciones a los movimientos de datos hacia el exterior del territorio nacional; es más, existe un problema en cuanto a la determinación del corpus jurídico (legislación vigente) aplicable en los casos en que los datos se almacenan y procesan fuera de la Unión Europea, o a través de un proveedor de servicios no perteneciente a la UE. Las cuestiones principales que deberá abordar cada uno de los organismos públicos y, más en general, cada una de las administraciones centrales de los países de la UE, son las siguientes:

- Si los marcos jurídicos actuales pueden modificarse de forma que faciliten la comunicación, el tratamiento y el almacenamiento de los datos en el exterior del territorio nacional sin que ello exponga la seguridad y privacidad de los ciudadanos y la seguridad y economía nacionales a riesgos inaceptables.
- En tal caso, si trasladar los datos de los ciudadanos al exterior del territorio nacional supone un riesgo asumible.
- Si el equilibrio entre los riesgos de perder el control sobre los datos y los efectos beneficiosos de la distribución geográfica es positivo para ellos.

Dichas consideraciones se aplican, en general, a todos los modelos de despliegue en la nube (es decir, públicos, privados, comunitarios e híbridos); aunque el impacto de estos puntos débiles y amenazas variará en función del entorno específico interno y externo de los organismos públicos en los distintos Estados miembros y del modelo de implementación y de distribución que se hubiese tenido en cuenta.

En términos de arquitectura, para el caso de aplicaciones sensibles, los modelos de nube privado y comunitario parecen ser la solución que mejor se ajusta en la actualidad a las necesidades de las administraciones públicas, ya que ofrecen el mayor grado de gobernanza, control y visibilidad, aun cuando, al planificar una nube privada o comunitaria, deba darse especial consideración a la escala de la infraestructura. Si una infraestructura de nube privada no alcanza la masa crítica necesaria, la mayor parte de los beneficios en cuanto a resistencia y seguridad del modelo de la nube no se aprovecharán.

Nos parece de especial interés el caso del modelo de nube comunitario, puesto que muestra el potencial de conjugar la gobernanza y controles de los datos y soluciones de IT con un alto nivel de resistencia, en especial, en el caso de una infraestructura de distribución y federada (v. anexo III).

La opción de la nube pública es capaz de ofrecer ya un servicio muy fiable y flexible con un nivel satisfactorio asociado de gestión segura de datos y, además, es la más rentable. Es más: la nube pública ofrece, potencialmente, el mayor grado de disponibilidad del servicio; aunque, debido a la actual complejidad normativa de las transferencias de datos transfronterizas, tanto intracomunitarias como extracomunitarias, su adopción deberá limitarse a aquellas aplicaciones no sensibles o no críticas y en el contexto de una estrategia definida para adoptar la nube, que deberá incluir una estrategia clara para el caso de abandono del modelo. Al mismo tiempo, ha surgido una serie de iniciativas, entre las que se incluyen la *CSA Guidance* (Directrices de la CSA) y otras dos iniciativas de la CSA, *Control Matrix* y *Consensus Assesment*, además de la labor del consorcio *Common Assurance Maturity Model* (CAMM) (2), que están impulsando el criterio de referencia en cuanto a ofrecer una transparencia y garantía que permitan usar el modelo de la nube pública en aplicaciones más sensibles.

Recomendaciones a las administraciones públicas y a los organismos públicos[1]

- Se recomienda a las administraciones públicas adoptar un método escalonado al integrar la computación en la nube en sus operaciones, puesto que la complejidad del entorno de la nube introduce una serie de variables desconocidas para las cuales los gestores públicos necesitarán crear nuevos métodos de evaluación y gestión de los riesgos.

  Los gestores públicos de cualquiera de los niveles de las administraciones deberán tener en cuenta la interconexión y las interdependencias (la mayoría de las cuales podrían desconocerse), sobre todo en el momento de trasladar de forma simultánea varios servicios a un sistema o sistemas de nube. Los gestores públicos deberán tener en cuenta esta cuestión en el contexto actual, en el que el entorno cambia de forma dinámica y nuestros conocimientos sobre la vulnerabilidad y los mecanismos de ataque, así como la complejidad de los controles relacionados, son incompletos. Por tanto, no deberán dar por sentado que la implementación con éxito de una aplicación en un entorno de la nube supone, de forma automática, un indicio positivo que aconseje llevar a cabo muchas otras implementaciones, sino que deberán examinarse de forma detenida e individual los requisitos de seguridad y resistencia de cada aplicación y compararse con las arquitecturas de la nube y los controles de

[1] *En el capítulo 7 puede verse la lista completa de recomendaciones*

seguridad ya disponibles. Ante tal perspectiva, deberá planificarse la capacidad de dar marcha atrás en la adopción de soluciones de computación en la nube antes de proceder a trasladarse a este modelo.

- Las administraciones públicas nacionales deberán elaborar, en el contexto de un planteamiento más amplio de la UE, una estrategia de computación en la nube que tenga en cuenta las implicaciones en cuanto a la seguridad y la resistencia que tendrán dichos modelos de prestación de servicios en el contexto de sus economías nacionales y servicios para los ciudadanos en la próxima década. Quienes los adopten en primer lugar en cada Estado miembro podrán ser percibidos como posibles bancos de pruebas, aunque será esencial contar, al menos en el ámbito nacional, con un planteamiento coherente y armonizado respecto a la computación en la nube con el fin de evitar: 1) la proliferación de plataformas y formatos de datos incompatibles (ausencia de interoperabilidad de servicios), 2) un planteamiento incoherente respecto a la seguridad y la resistencia, incluido un planteamiento incoherente e ineficaz respecto a la gestión de riesgos y 3) la ausencia de masa crítica.

- Recomendamos a las administraciones públicas que estudien el papel que desempeñará la computación en la nube en el contexto de la protección de las infraestructuras críticas de la información. No resulta descabellado pensar que la computación en la nube, en todas sus posibles implementaciones, prestará servicio, en un futuro cercano, a una parte significativa de ciudadanos, pequeñas y medianas empresas y administraciones públicas de la Unión Europea y, por tanto, las infraestructuras en la nube desde las que se prestan dichos servicios deberán disponer de protección. En otras palabras, las estrategias nacionales de computación en la nube deberán dirigirse a comprender y abordar, entre otras cuestiones, los efectos de la interoperabilidad e interdependencias de las nubes nacionales y supranacionales, así como a evaluar el impacto de posibles fallos en cascada, evaluar la oportunidad que supondría incluir a los proveedores de la nube en el ámbito de los ya anunciados planes de generación de informes (en particular, nos referimos al mecanismo de generación de informes que introducen los artículos 4 y 13 de la recientemente adoptada Directiva 2009/140/CE (3)) y prepararse para posibles gestiones de crisis en caso de producirse incidentes a gran escala de esta índole.

- Recomendamos a las administraciones públicas nacionales y a las instituciones de la Unión Europea que continúen investigando el concepto de una nube gubernamental europea como un espacio virtual supranacional en el que pueda aplicarse un conjunto de normas coherente y armonizado, tanto en términos de legislación como de medidas de seguridad, en donde puedan promoverse la interoperabilidad y la estandarización. Además, una infraestructura de la Unión Europea de esta amplitud podría emplearse en el contexto de un plan de ayuda y asistencia mutuas paneuropeo para casos de emergencias.

Al evaluar los beneficios y riesgos de adoptar la computación en la nube, los organismos públicos deberán llevar a cabo las acciones siguientes:

- Evaluar sus riesgos y definir sus requisitos (posiblemente, utilizando como base los que se sugieren en este informe) para identificar la solución de nube que mejor se adapte a sus necesidades. Los gestores públicos deberán tener en cuenta también los factores humanos (tales como la concienciación sobre la seguridad y la resistencia, o la resistencia a los nuevos modelos de medidas de seguridad) y los marcos normativos.

- Revisar sus políticas y procesos existentes de gestión de la seguridad de la información y evaluar de qué modo se abordarían o apoyarían éstos en diversos modelos de nube.

- Definir los niveles de servicio que resulten aceptables (una referencia para evaluar parámetros como la disponibilidad, tiempo de respuesta, etc.) para sus requisitos. Usarán la referencia o referencias para medir el desempeño de sus servicios. Identificar el conjunto de controles y el grado de especificidad de éstos que sea necesario para alcanzar un nivel mínimo aceptable de gestión segura de datos y la resistencia de los servicios.

- Asegurarse de que todos los requisitos fundamentales de seguridad, resistencia y jurídicos se especifiquen en sus requisitos de nivel de servicio y se concreten en sus acuerdos de nivel de servicio.

- Disponer de herramientas, metodologías y estructuras de gobernanza de cara a, por ejemplo, asegurar la debida diligencia.

- Asegurar que se garanticen y mantengan conexiones de telecomunicaciones satisfactorias, las instalaciones de servicio críticas (p. ej., la electricidad), la potencia de procesamiento y la capacidad de almacenamiento.

  Comprobar la prioridad para la reanudación de las comunicaciones y los servicios en la nube de terceros en caso de interrupción.

- Examinar el plan de continuidad del negocio junto con la cadena del suministro de los servicios.

Por último, los proveedores de la nube y los proveedores de servicios independientes deberán considerar las recomendaciones que se incluyen en este informe como posible fuente de información a la hora de alinear sus ofertas comerciales y propuestas de valores con las necesidades y requisitos de los usuarios.

Introducción

Muchos ministerios, organismos gubernamentales y administraciones públicas (AAPP) fuera de la Unión Europea, p. ej., de los Estados Unidos o Japón[2], Singapur (4), y muchos otros países, se están planteando en la actualidad las posibilidades de la nube.

Las principales razones de esta elección se exponen de forma minuciosa en el documento *State of Public Sector Cloud Computing*, del Federal Chief Information Officer de Estados Unidos, que dice: «[...] la computación en la nube tiene el potencial de reducir notablemente la mala gestión de recursos, aumentar la eficacia de los centros de datos y las tasas de utilización, y disminuir los costes de explotación...». En la Unión Europea (5), algunos países, como el Reino Unido, Dinamarca y los Países Bajos, además de la Comisión Europea (6) (7), están analizando el modelo de computación en la nube y trabajando en la definición de sus estrategias.

En mayo de 2010, la Comisión Europea publicó su Agenda Digital para Europa (8), en la que se comunica lo siguiente: «[…] la Comisión garantizará el respaldo económico suficiente a las infraestructuras de investigación de las TIC conjuntas y a los grupos de innovación, desarrollará más infraestructuras electrónicas (*eInfrastructures*) y establecerá una estrategia europea de computación en la nube, en especial, en el caso de las administraciones públicas y en el campo científico».
Al mismo tiempo, en el sector privado, el número de empresas que usan la nube continúa aumentando a un ritmo acelerado y el desarrollo de las ofertas está aumentando con la introducción de nuevos servicios.

Según Gartner, la previsión de beneficios de los servicios en la nube alcanzaría los 68.300 millones de dólares en 2010, lo que supondría un aumento del 16,6 % con respecto al de 2009, que fue de 58.600 de millones de dólares. Se prevé un crecimiento en el sector para el 2014, año en el que el beneficio de los servicios en la nube podría alcanzar, según se estima, los 148.800 millones de dólares.
Teniendo en cuenta las medidas citadas anteriormente y el contexto de la actividad de negocio, ENISA considera importante ofrecer directrices respecto a los factores de seguridad y resistencia que influyen en la opción por (o la decisión en contra de) las soluciones de computación en la nube para organismos y organizaciones de carácter público. Por esta razón, hemos decidido respaldar a los organismos públicos mediante una evaluación comparativa de los distintos planteamientos respecto a la computación en la nube.

Este informe es una continuación del informe publicado en 2009 por ENISA *Cloud computing: benefits, risk and recommendations for information security*, donde se llevó a cabo una evaluación de riesgos de

[2] En Japón, el ministerio de Asuntos Interiores y Comunicación (MIC) está creando la *Kasumigaseki Cloud* para optimizar operaciones en los gobiernos centrales. El ministerio de Economía, Comercio e Industria (METI) ha creado la *J-SaaS* y la *e-METI Idea box*. Hay varios proyectos de nube, o ya existentes, o planeados, en los sectores público y empresarial, como el sector financiero, las líneas aéreas, las comunicaciones, el agua y otros proyectos.

los modelos de negocio y las tecnologías de la computación en la nube. El resultado es un análisis independiente y en profundidad que expone, de forma general, algunos de los beneficios de la seguridad de la información y riesgos clave de seguridad de la computación en la nube. El informe ofrece también una serie de recomendaciones prácticas.

Ambos informes, *Governmental Cloud: making an informed decision* y *Cloud Computing: benefits, risks and recommendations for information security* se elaboraron en el contexto del Programa Emerging and Future Risks (Riesgos emergentes y futuros).
Véanse otros trabajos de ENISA en el campo de la resistencia en (9).

1.1. Estructura del informe y guía de lectura

El informe se estructura del modo siguiente:

En el capítulo 2 se describen los objetivos del informe, el método de análisis y los destinatarios.

En el capítulo 3 se presenta un modelo sencillo para los responsables de la toma de decisiones y se describen los tres primeros pasos del proceso: identificación de los parámetros de seguridad y resistencia (paso 2), identificación de los parámetros de funcionamiento y jurídicos (paso 1) y, por último, las opciones disponibles de arquitectura para los servicios de TI (paso 3). Cabe señalar que dichos pasos no aparecen en su orden de secuencia lógico: presentamos al lector en primer lugar el paso 2 y, a continuación, el paso 1, lo cual se debe a que la seguridad y la resistencia son las cuestiones a las que se dirige el informe.

En el capítulo 4 se describe el cuarto paso del modelo, es decir, la evaluación comparativa, y se presenta un análisis general DAFO (en inglés, SWOT) de modelos de nube comunitario, privado y público.

En el capítulo 5 se ofrece una demostración sobre la forma de aplicar los cinco primeros pasos del modelo sencillo para la toma de decisiones a través del análisis de cuatro ejemplos de servicios que se extraen de las tres situaciones hipotéticas estudiadas en el informe.

En el capítulo 6 se describen las actuaciones que deberán llevarse a cabo y los controles que deberán tenerse en cuenta en relación con la seguridad de la información y la resistencia del servicio a la hora de elaborar las solicitudes de propuestas de servicios.

En el capítulo 7 se proponen una serie de recomendaciones en materia de seguridad de la información y resistencia del servicio para la evaluación por parte de las administraciones públicas y organismos públicos nacionales de las opciones de computación en la nube.

Por último, se han incluido como anexos los documentos siguientes:

- Anexo I: Análisis jurídico.
- Anexo II: Situaciones hipotéticas.

- Anexo III: Arquitectura del Proyecto Reservoir.
- Anexo IV: Lista de amenazas, que sirve de documento de apoyo para la elaboración de una evaluación de riesgos en profundidad.

Dado que el informe tiene diversos destinatarios, el lector deberá tener en cuenta los aspectos siguientes:

- La información esencial se incluye en la parte del resumen y de las recomendaciones clave, al principio del informe.
- La información no destinada a expertos se ha elaborado en forma de relato y se encuentra en la situación hipotética introductoria.
- El análisis pormenorizado se encuentra en la parte principal del informe.
- El análisis en profundidad se encuentra en los anexos.

1.2. Situación hipotética introductoria: Tomar una decisión

El Ministro de Comunicaciones y Tecnología fruncía el ceño y golpeaba con la punta de los dedos, impacientemente, la bruñida mesa del despacho cuando su ayudante abrió la puerta y entró, junto con su equipo de trabajo. El ayudante hizo las presentaciones de rigor: Paulo y Hardizon, del sector privado; Apik, un abogado particular; Hitch, Jefe del departamento ministerial de TI; Luther, Consejero General del Ministro; Fudge, Jefe de la Oficina Económica del Ministro; Veeraswami, una auditora independiente.

—Esta situación me desagrada, señores —hizo una pausa y asintió hacia Veeraswami—, y señora. Me decepciona que no hayan sido ustedes capaces de llegar a un consenso respecto a si debería recomendar o no al Primer Ministro el traslado de los servicios de informática del gobierno a la nube. Hitch puso con mucho cuidado encima de la mesa del Ministro un informe de 300 páginas y lo movió hacia donde estaba éste. —Aquí están todas las reflexiones del equipo de trabajo, las ventajas e inconvenientes.

La Ayudante del Ministro, Ference, se inclinó hacia Hitch y le susurró: «Ya sabe que el Ministro no lee nunca nada que pase de dos folios».

—Bueno, pues, entonces —dijo Hitch—, le puedo hacer un resumen de todo el informe, señor. Siento tener que decir que hay división de opiniones, a partes iguales, en el equipo de trabajo; tendrá usted que tomar la decisión.

El Ministro miró su reloj. —Pues es un engorro, la verdad. Bien, entonces, díganme cuáles son los aspectos clave. Primero, ¿en cuánto reduciríamos los gastos en TI si nos trasladásemos a la nube?». —En mucho, señor Ministro —intervino Fudge—, en torno a un noventa por ciento. Hay mucha duplicación en los departamentos del gobierno: Cada institución pública tiene su propio departamento de TI, es decir, personal que ejerce las mismas funciones, así como sus propios servidores. A veces utilizan servicios propietarios y otras, servicios de disposición pública. Si consolidamos todo nuestro almacenamiento y servicios en la nube, ganaremos en eficacia operativa. No necesitaríamos autorizar licencias para el mismo software muchas veces para cada departamento. Podríamos reducir el tamaño de los departamentos de TI y disminuir los gastos en TI en unos 30.000 millones de euros al año (10). Pagaríamos el servicio que realmente usamos, en vez de estar pagando cosas que, luego, puede que usemos o no. Además, podríamos contarlo como gasto de explotación en vez de como gasto de capital, con lo que mejoraríamos el aspecto de las partidas del presupuesto.

—Al departamento de TI también le corresponderían beneficios —añadió Hitch—. Si usamos la nube como banco de pruebas y desarrollo, se reducirían en gran medida el tiempo y el coste del desarrollo del nuevo servicio. No tendríamos que esperar a las entregas de nuevas máquinas, ni necesitaríamos preparar estimaciones de picos de capacidad de carga, porque la nube es escalable por su propia naturaleza. Lo que hace la nube es proporcionar al personal agilidad en la preparación de nuevos servicios.

—Excelente —dijo el Ministro, esbozando un sonrisa de satisfacción—. Entonces, ¿dónde está el problema? ¿Por qué no han llegado a un consenso?»

Veeraswami sonrió con serenidad. —Respecto al ahorro considerable en los costes no hay dudas —afirmó—, pero no se trata de una mera cuestión de ahorro. Los beneficios podrían ser importantes. Hay ciertos, digamos... costes y aspectos ocultos que también hay que tener en cuenta…»

—¿Por ejemplo? —preguntó el Ministro.

—Modificaciones de las aplicaciones ya existentes, recuperación de desastres, responsabilidad legal, pérdida de control inmediato, contrataciones de seguros para cubrir posibles pérdidas de datos… y, quizá, lo más importante, en caso de que los proveedores de los servicios de la nube no fuesen europeos, se perdería la oportunidad de desarrollar las capacidades nacionales, de modo que también habría un coste de oportunidad.

—Los costes de oportunidad y los intangibles no se pueden trasladar fácilmente a los votantes —se quejó el Ministro.

—No es solo cuestión de costes —interrumpió Apik—. El gobierno perdería el control de todos sus datos, de los datos de todos sus ciudadanos. No tendría ni idea de dónde habrían ido a parar los datos. Podrían estar en cualquier parte del mundo. Podrían haberse almacenado en un país donde no se cumple la Directiva de Protección de Datos. Imagine la reacción de la prensa si descubriesen que se está haciendo en otro país que no es seguro un minado de todos sus datos, secretos de estado y datos personales. El escándalo podría hundir a su gobierno.

—Bueno, bueno —dijo Hardizon—, no hace falta exagerar. Solo usaríamos nuestras instalaciones por las vías permitidas legalmente, y la legislación comunitaria nos permite cierto grado de resistencia. A ninguno nos interesa que nuestros datos vayan a parar a un lugar inadecuado, y hay solo un número limitado de países en donde disponemos de las instalaciones adecuadas, de todas formas.

—Estoy completamente de acuerdo, señor Ministro —dijo Luther—. Es una cuestión contractual. El gobierno podría disponer de un contrato en el que se especificase en qué lugares podrían o no almacenarse los datos. Tendría que ser un lugar de la Unión Europea.

—Claro, claro... —dijo Apik—. Pero no habría forma de saber si se está cumpliendo o no el contrato. Es cierto —dijo Veeraswami—. A partir de nuestro estudio, es imposible saber dónde están los datos, o a dónde van a parar.

Hardizon resopló. —Eso no es verdad. Podemos alcanzar un acuerdo de nivel de servicio para que la copia de seguridad de los datos se conserve exclusivamente en Europa.

Pero la cuestión es que no hay forma de auditar el cumplimiento debido del contrato, de saber dónde están los datos en un momento dado o quiénes tienen acceso a ellos o qué medidas de seguridad están vigentes para protegerlos.

Tendríamos cierto conocimiento, pero no todos los elementos de juicio. Esto se debe a que nuestros sistemas son propietarios» —dijo Paul—. Mi empresa, por ejemplo, cuenta con un historial en el sector que es la envidia de nuestros competidores. No vamos a renunciar de ningún modo a nuestra ventaja competitiva.

—Puede ser —dijo Hitch—, pero, si hubiese alguna incidencia, la que fuese, en la nube A o si sus servicios no resultasen satisfactorios y quisiéramos cambiar a una nube B, nos resultaría prácticamente imposible, porque sus sistemas son propietarios, lo cual es otra forma de decir que no son interoperables. Y ésa es mi principal preocupación. Estaríamos atados a un proveedor específico.

—Sí —dijo Apik—. ¿Qué les parecería eso a los votantes?

— ¿Quiere decir —preguntó el Ministro— que si optásemos por un proveedor, y no estuviéramos satisfechos con el servicio prestado, o se produjesen incidencias, no podríamos trasladar nuestro negocio a otro sitio?

—No exactamente, señor Ministro. La mayoría de los proveedores tienen interfaces de programación de aplicaciones, o API, que es como se las suele llamar, lo cual significa, básicamente, que no es sencillo portar las aplicaciones de una nube a otra.[3]

—Mmm, pues eso no suena muy bien... —caviló el Ministro, mientras se frotaba la barbilla—. Quizá sea necesario promulgar una nueva normativa, así los proveedores estarían obligados a estandarizar esas... ¿Cómo las ha llamado? ¿API?

—Es posible que las API no sean las mismas, pero, siempre que sean abiertas, es factible insertar bibliotecas sencillas para hacer la portabilidad. Si quieren que nos estandaricemos demasiado pronto, lo que se consigue es matar la innovación por parte de nuevos competidores, entre ellos, nuestra futura competencia de la UE. Además, los actuales sistemas a medida tienen restricciones mucho más serias, que es por lo que tienen tantos problemas. Pero seamos sinceros —pidió Paulo, tratando de cambiar el rumbo del debate—. Es una cuestión de coste y de disponibilidad. Nuestros servicios y sus datos estarían disponibles, más o menos, todo el tiempo. Ofrecemos el 99,5 % de disponibilidad, mientras, por algunas cifras que he podido consultar, los servicios del gobierno ni se acercan...

—Cierto, la misma que ofrecemos nosotros —dijo Hardizon, que no deseaba quedar por debajo de la competencia. Los gobiernos suelen emprender grandes proyectos de TI que tropiezan con dificultades. Los planes y los costes suelen quedar desbordados. Si se cambiasen a nuestra nube, podría cargar

[3] *«En la actualidad no existe normalización, y tampoco se ha hecho un esfuerzo concertado por parte de los proveedores de servicios en la nube para desarrollar una programación de aplicaciones ubicua y sistemática entre nubes (lo que supone que portar de una nube de PaaS (Plataforma como Servicio) a otra resulte una tarea ingente.» Mather et al., pág.*

sobre nuestros hombros ese riesgo». Hardizon se enderezó y estiró los hombros, como si quisiera ilustrar su argumento.

—Mi empresa no ofrece una simple copia de seguridad, sino varias —dijo Paulo—, y en distintos países, por ejemplo, en Europa y en los Estados Unidos. Los gobiernos no hacen eso. Si hubiese un fallo masivo en el suministro energético, como el que se produjo en Alemania hace unos años[4] y éste provocase un efecto en cascada hasta España y Portugal, podríamos hacerle frente. Es decir, que no nos jugamos todo a una carta, tenemos varias cartas.

—Con su permiso, señor Ministro —dijo Luther—, quisiera decir que, aunque tener las localizaciones geográficamente dispersas ayuda a asegurar la resistencia en caso de cortes de suministro energético como el de Alemania, esto plantea ciertos problemas de jurisdicción. Podríamos encontrarnos con que no hay acuerdos de puerto seguro vigentes suscritos con algunos de esos terceros países, y que, por tanto, los datos de nuestro gobierno estarían sometidos a lo que dijese la legislación y normativa de otros países.

—Exacto —dijo Apik—. Los proveedores de servicios en la nube operan en muchas jurisdicciones distintas de forma simultánea. No podríamos evitar que llevasen a cabo la práctica de buscar el régimen jurídico más conveniente.

A Luther no le sentó bien que lo interrumpieran, pero, como Apik lo había hecho para respaldarlo, le sonrió ligeramente y siguió exponiendo sus argumentos. —Y pudiera ser —continuó— que no pudiese evitarse de ninguna forma que las autoridades competentes accediesen a los datos…

—Además, los propios proveedores de la nube podrían hacer un minado de los datos —dijo Apik—. Imagine el tesoro oculto que serían los datos de un gobierno...

—Eso es un disparate —dijo Paulo—. Es incluso insultante.

—Disculpe —respondió Apik—. Entiendo que su reputación es realmente valiosa y que no obtendrían ningún beneficio echándola por tierra, que es lo que pasaría si se hiciera un minado de los datos de los particulares, pero un proveedor sin escrúpulos podría plantearse hacer algo así.

—Puede ser, pero es el mismo riesgo que existe con las empresas a las que se paga para generar y escribir software y gestionar los centros de datos ya existentes; el riesgo, de hecho, es incluso mayor en este caso, ya que ustedes están deteriorando el modelo de negocio de estas empresas por el mero hecho de plantearse la opción de los sistemas de nube reales. Estoy de acuerdo en lo de que es necesario tener en cuenta los riesgos, pero, ¿por qué íbamos a destruir un valioso modelo de negocio comportándonos de forma tan estúpida?»

---

[4] *Graham, Dave, y Allan Hall: "Power cuts in Germany spark wave of blackouts across Europe"*, The Scotsman, *6 nov 2006. http://news.scotsman.com/international.cfm?id=1640182006*

—Hay otro problema —añadió Apik—. ¿No es cierto que, como resultado de la promulgación de la Patriot Act norteamericana, el gobierno canadiense dio la orden a sus departamentos de no usar ordenadores que operasen dentro de las fronteras norteamericanas porque les preocupaba la confidencialidad y privacidad de los datos canadienses almacenados en esos ordenadores?».[5]

Ference, Ayudante del Ministro, viendo que se volvían a caldear los ánimos entre los miembros del equipo de trabajo, trató de rebajar algo la tensión: —Quizá convendría que informasen al Ministro sobre la cuestión de la resistencia del traslado a la nube.

—Buena idea —dijo Hardizon—. Señor Ministro, la resistencia no es solo una cuestión de tener centros de datos separados ampliamente. El hecho es que contamos con algunos de los mejores expertos en seguridad del mundo trabajando para garantizar que solo el personal autorizado tenga acceso a nuestros sitios y sistemas. Es prácticamente imposible vulnerar nuestra seguridad con un ataque, sea físico o desde el ciberespacio.

—Solo que esto ya ha sucedido… —dijo Hitch—. En cualquier caso, debe preocuparnos la seguridad de los datos desde el momento en el que se generan y durante el tránsito a la nube y el hecho de tener acceso a ellos las 24 horas del día, siete días a la semana, 52 semanas al año. No hay sistema de seguridad perfecto. Al centralizar los servicios y el almacenamiento, el riesgo será que se tendrá un objetivo de mayor tamaño que atacar.

—Estoy de acuerdo en que no hay sistema de seguridad perfecto, pero los sistemas del gobierno sufren ataques y son vulnerados con más frecuencia, incluso. Podríamos suponer un objetivo de mayor tamaño, pero no olvidemos que podríamos crear, también, defensas más potentes y profundas de lo que podría nunca, ni siquiera plantearse, cada departamento individual de TI por separado, como ya señaló ENISA el año pasado: el tamaño favorece la seguridad —dijo Paulo.

—Es posible, pero los proveedores de los servicios de la nube tendrán que enfrentarse con delincuentes, clientes malintencionados y amenazas internas, como cualquier otra organización —dijo Hitch.

—Es verdad —dijo Paulo—, pero también examinamos a nuestros futuros empleados de forma más rigurosa de lo que lo hace el gobierno. Y, teniendo en cuenta cómo funcionan nuestros sistemas, hay muchas menos personas que intervienen en la gestión de nuestros sistemas de las que tienen acceso a los datos en sistemas que gestionan ustedes.

— ¿Y quién les examina a ustedes? —preguntó el Ministro.

Apik, aprovechando la ocasión, intervino otra vez. —Buena pregunta, señor Ministro. Es conocida la falta de transparencia en relación con las medidas de seguridad de los proveedores de los servicios de la nube. Esperan que los clientes les confíen sus datos valiosos y, a veces, críticos, pero nadie sabe qué

[5] *Mather, Tim, Subra Kumaraswamy y Shahed Latif,* Cloud Security and Privacy, *O'Reilly Media, Sebastopol, CA, 2009, pág. 33*

medidas aplican para proteger esos datos. La falta de transparencia significa, al final, falta de confianza; o, al menos, así me lo parece a mí.

— ¿Y bien, señores Harizon y Paulo? ¿Qué dicen a eso?».

—Pues es muy sencillo, señor Ministro —dijo Paulo—, si me permite la expresión. No queremos que las medidas de seguridad que hemos puesto en marcha puedan caer en manos de personas que, potencialmente, puedan llevar a cabo ataques: No revelamos nuestras medidas de seguridad para poder así protegerles mejor a ustedes y al resto de nuestros clientes.[6]

—La solución son las auditorías de terceros independientes —dijo Veeraswami, la auditora independiente.

—Las auditorías son importantes, en eso estoy de acuerdo —dijo Luther—, pero son los acuerdos de nivel de servicio (ANS), contratos firmes como pilares, lo que de verdad necesitamos para solucionar esto.

—Lo son —coincidió Apik—. Pero los proveedores de servicios de nubes comerciales normalmente solo ofrecen contratos con clausulado estándar: lo tomas o lo dejas. Las oportunidades de negociar cláusulas individuales son extremadamente reducidas».

El Ministro volvió a refunfuñar. —Pues si quieren hacer negocios con nosotros, habrá que negociar un contrato que nos satisfaga a nosotros, y que a la gente le parezca satisfactorio… y, además, siempre podremos recurrir a promulgar regulaciones y normas. Quien quiera operar en nuestro país, tendrá que ajustarse a nuestros criterios y cumplir nuestra regulación.

Hardizon asintió con la cabeza. —Por supuesto, señor Ministro, por supuesto.
Normalmente, discrepo de mi amigo Hardizon, señor Ministro, pero, en este caso, suscribo lo que acaba de decir. Eso sí, no obstante, me gustaría recordarle que el compromiso de su gobierno es con una mejor regulación, con menos regulación y con libertad de empresa.

Señor Ministro, no tiene por qué hacer la recomendación al Primer Ministro de migrar o bien todos los datos y servicios del gobierno a una nube, o ninguno: podría recomendar un planteamiento por fases —sugirió Hitch.

—Continúe.

—Quiero decir que podríamos hacer la migración de algunos datos y servicios, pero no de todo al mismo tiempo. Eso sería, de hecho, muy arriesgado. Sería mejor hacer la migración de algunos datos y servicios. Cosas que no sean esenciales, es decir, datos que no sean críticos, como, por poner un

[6] *No obstante, en el caso de clientes que son empresas, deberá exigirse transparencia a los proveedores de los servicios de la nube y solicitar la información necesaria para efectuar la evaluación de riesgos y demás gestiones de seguridad que se precisen en los sucesivo.» Mather et al., pág.*

ejemplo, turismo y obras públicas. Gracias a la experiencia obtenida en esa primera fase de la migración, podríamos tomar con más criterio la decisión de si, en la segunda fase, seguir adelante con la migración de datos más sensibles, por ejemplo, los datos de servicios sociales y sanidad.»

—Bien, me gusta esa idea. Echó una mirada a los presentes. —¿Consenso? ¿Sí? Pues hecho.

El Ministro ya iba a despedirse del equipo de trabajo (tenía una agenda muy apretada), pero, antes de que pudiera hacerlo, Hitch intervino: —Señor Ministro, creo que es un muy buen resultado el que ha logrado usted aquí hoy, pero, si me permite, hay una o dos cuestiones pendientes de aclarar.

El Ministro, que ya se había dado por satisfecho con el aparente acuerdo, volvió a fruncir el ceño: —¿Sí? ¿De qué se trata?

—Bueno, creo que, desde el sector, deberían asegurarnos que se aplican ciertos mecanismos de seguridad, por ejemplo, cifrado de seguridad, firmas digitales, métodos de dispersión tipo *hashing*, etc., que garanticen un grado satisfactorio de confidencialidad, integridad, disponibilidad y no repudio».

El Ministro no estaba seguro de qué podría querer decir todo aquello, pero parecía razonable.
—Estoy de acuerdo, señor Ministro —dijo Luther, el Consejero General—. Necesitamos un contrato en el que se especifiquen tanto la seguridad de los datos como la resistencia del servicio, aunque, también, un acuerdo en donde se establezca de forma clara cuál sería la jurisdicción competente y en qué circunstancias y a qué clase de datos podría tenerse acceso.

—Pues está claro: sería nuestra jurisdicción —dijo el Ministro.

—Sí, por supuesto —dijo Luther—. Pero no es tan sencillo. Si acordamos que el proveedor de servicios de la nube almacene la copia de seguridad de nuestros datos en Islandia, en Canadá o cualquier otro sitio, tendríamos que tener un acuerdo ejecutable en el que se especificasen los tipos de datos y qué servicios pueden transferirse fuera de nuestras fronteras. Deberíamos establecer un nivel de gestión segura para cada categoría de datos y servicios. En términos concretos, eso supondría que los datos sensibles podrían transferirse fuera de de nuestras fronteras solo en el caso de que se cumplieran ciertos requisitos.

El Ministro se rascó la cabeza. —Sí, me parece correcto.
Luther prosiguió. —Si acordamos la transferencia de los datos de nuestros ciudadanos a un tercer país, esto implicaría la existencia de una sólida relación de confianza entre ambos gobiernos. Sin embargo, es posible que necesitemos algo más que eso. Haría falta un tratado internacional que ofreciese pleno control sobre la situación de los datos y sobre la jurisdicción. Se necesitaría un acuerdo bilateral o multilateral entre nuestro gobierno, el Estado en el que se conservase la copia de seguridad y el gobierno del país en el que el proveedor de servicios de la nube tuviese su sede principal a efectos legales. Ese acuerdo debería incluir disposiciones que estipulen la regulación de citaciones judiciales y la obtención de datos para fines judiciales (*e-discovery*).

Apik añadió algo más. —Señor Ministro, esto no afecta solo a los factores técnicos o jurídicos, sino que, además, deben tenerse también en cuenta los factores humanos.

—Hmm —dijo el Ministro—. Pues parece que sí hay muchos factores que hay que tener en cuenta… Hitch intervino. —Es verdad, señor Ministro, sí que los hay. Por suerte, esta misma mañana he recibido un informe de ENISA….

— ¿ENISA?

—Sí, señor Ministro, ya sabe, la Agencia Europea de Seguridad de las Redes y de la Información —aclaró su ayudante.

—Sí, por supuesto. ¿Y…?

—Y, precisamente —dijo Hitch—, se tratan estas mismas cuestiones.

—Excelente — dijo el Ministro—. Estúdienlo detenidamente y adelante con ello.

Todo el equipo de trabajo asintió y coreó, al unísono: «Sí, señor Ministro».

Objetivos y análisis

El objetivo de este informe es doble: 1) Orientar a los organismos públicos tanto en la definición de sus perfiles de seguridad de la información y resistencia como en la evaluación de los puntos fuertes, puntos débiles, oportunidades y amenazas del NIS (*Network Information Service*, Sistema de Información en Red) de los modelos de prestación de servicios de computación en la nube y, 2) ofrecer respaldo de forma indirecta a los Estados miembros en la definición de sus estrategias de nube nacional en relación con la seguridad de la información y la resistencia del servicio.

Los organismos públicos podrán encontrar en el informe ideas y herramientas pensadas para facilitarles la respuesta a las cuestiones siguientes:

- ¿Qué valor tiene una solución de nube pública en cuanto a resistencia y fiabilidad?
- ¿Tiene el modelo de prestación de servicios en la nube posibilidades de ofrecer, al menos, el mismo nivel de seguridad y resistencia que el modelo que tienen actualmente las organizaciones públicas (autoridades públicas locales y regionales y autoridades sanitarias)?
- ¿Qué modelo de implementación (privado, público, híbrido, o comunitario) se adapta mejor a las necesidades de una administración pública en particular, en caso de que alguno de ellos se adecue?
- ¿Cuál de las combinaciones entre modelos de servicios (IaaS [Infraestructura como servicio], PaaS [Plataforma como servicio], SaaS [Software como servicio] y servicios (p. ej., recopilación en línea de historias clínicas, pago de impuestos en línea y otros servicios menos críticos, como servicios administrativos (*back-end*), recursos humanos, nóminas o la formación en red (*e-learning*) es la mejor, si es que alguna lo es?
- ¿De qué modo pueden las administraciones públicas asegurar controles efectivos sobre la seguridad y la resistencia? ¿Qué formas de auditorías, acuerdos de nivel de servicio, sanciones económicas o incentivos, etc., serán más eficaces a la hora de proporcionar el aseguramiento adecuado?
- ¿Sobre quién recae la responsabilidad, y en relación con qué aspectos, de las medidas relativas a la seguridad y resistencia en una implementación típica de nube gubernamental?
- ¿Qué normas y regulaciones deben seguirse? ¿Qué deberes y qué obligaciones deben observarse?
- ¿Sería realista que las administraciones públicas planifiquen e implementen nubes gubernamentales con la tecnología de la que se dispone actualmente? ¿Cuáles son las

principales cuestiones abiertas que deben abordarse en términos de seguridad y resistencia con carácter previo a que la nube gubernamental pueda implementarse y operar?

1.3. Destinatarios

Los destinatarios del informe son los siguientes:

- Directores ejecutivos (CEO), directores de Tecnología (CTO) y directores de Seguridad de la Información (CISO) y otro personal de los departamentos TIC en los Estados miembros de la UE que evalúen la seguridad de la información, resistencia y fiabilidad de una nube gubernamental.

- Organismos públicos de la UE (administraciones públicas locales y regionales, agencias, autoridades sanitarias locales, etc.) que evalúen los costes y beneficios que acarrearía a una administración pública la opción de migrar a una nube.

- Responsables de elaboración de políticas de la Unión Europea a los que correspondan las decisiones relativas a las medidas oportunas e incentivos económicos, medidas legislativas, iniciativas de concienciación, etc. respecto a las tecnologías de computación en la nube para gobiernos y administraciones públicas.

- Proveedores de nube y proveedores de SVA (servicios de valor añadido, incluida la seguridad) que deseen obtener una primera idea acerca de las necesidades y requisitos de los gobiernos centrales, administraciones públicas y particulares.

1.4. Método de análisis

El presente informe incluye tres casos prácticos o situaciones hipotéticas que describen:

- El caso de una autoridad sanitaria local que introduce historias clínicas electrónicas y otros servicios electrónicos. Este ejemplo pretende mostrar los requisitos de aquellos servicios que se enfrenten al tratamiento de datos más sensibles y necesidades de resistencia más estrictas.

- El caso de una administración pública local que extiende nuevos servicios a los administrados y desarrolla los ya existentes a la vez que consolida sus infraestructuras y plataformas internas de TI.

- El caso de una administración pública central que planea la creación de una nube gubernamental para servir de plataforma secundaria que estimule la innovación empresarial.

Los datos a partir de los cuales se concibieron y elaboraron las tres situaciones se extrajeron de:

- Cinco autoridades sanitarias locales (Italia).

- Una autoridad sanitaria nacional (Países Bajos).
- Una administración pública local (España).
- IPA – Information Technologies Promotion Agency (Agencia para la Promoción de las Tecnologías de la Información), Japón.
- ELANET (CEMR) - Red Europea de eGobierno y Sociedad de la Información (con el respaldo del Consejo de Municipios y Regiones de Europa).
- Una autoridad de protección de datos (Grecia).
- Un cuestionario distribuido a fuentes cualificadas de las administraciones públicas.
- Una consulta abierta en línea.

A la fase de definición de las situaciones (las tres situaciones se encuentran en el Anexo II) le siguió el análisis, que incluyó los pasos siguientes:

- Definición de un modelo sencillo para responsables de la toma de decisiones.
- Identificación de los requisitos y restricciones empresariales, de funcionamiento y jurídicos.
- Alineación de los requisitos relacionados con la seguridad de la información y la resistencia con los requisitos empresariales, de funcionamiento y jurídicos.
- Descripción de las opciones disponibles de arquitectura de TI.
- Análisis de los puntos fuertes, débiles, oportunidades y amenazas de modelos de servicios de nube basados en parámetros de seguridad y resistencia.
- Identificación de los requisitos específicos de seguridad, resistencia y cumplimiento de los cuatro (4) ejemplos de servicios que se describen en las tres (3) situaciones.
- Evaluaciones comparativas, específicas para casos hipotéticos (basadas en el análisis DAFO) de modelos de implementación de computación en la nube.
- Definición de recomendaciones, lo que incluye una serie de controles o cuestiones que deberían usarse tanto en la fase de diseño de un servicio como en la supervisión del cumplimiento del acuerdo de nivel de servicios.

Modelo para responsables de la toma de decisiones

En este capítulo se propone un modelo sencillo que sirva de apoyo a los responsables públicos de la toma de decisiones a la hora de plantearse un modelo de prestación de servicios de computación en la nube. La idea es orientar a las administraciones públicas en lo siguiente:

- Identificación y recopilación de sus requisitos empresariales, de seguridad y jurídicos.
- Definición de sus especificaciones de nivel de servicios y acuerdos de nivel de servicios.
- Identificación de la solución que mejor aborde sus necesidades.
- Preparación de una propuesta de solicitud de servicio y establecimiento de su plan de mitigación.

En la descripción del modelo sencillo para los responsables de la toma de decisiones, destacamos la importancia de la fase de recopilación de requisitos, que es un factor clave en la adopción de la decisión fundada definitiva.

En términos generales, podemos afirmar que la aplicación de nuevos servicios de nube pública y la evolución de los ya existentes están condicionadas por lo siguiente:

Entorno interno

- Requisitos de la misión y de la actividad de negocio.
- Limitaciones financieras.
- Situación actual.

Factores externos

- Opciones de tecnología disponibles.
- Expectativas de los usuarios (ciudadanos, empresas privadas, pacientes, etc.) y la opinión pública.
- Legislación y normativa existentes tanto en el ámbito nacional como en el de la Unión Europea.

Las variables mencionadas deberán tenerse en cuenta al alinear una estrategia de seguridad de la información con los objetivos de negocio de una institución pública. Éstas deberán ser las guías principales a la hora de definir un perfil de riesgo para una organización pública y, por consiguiente, a la hora de determinar el nivel de madurez en la seguridad de la información y la resistencia que la organización necesita para la provisión del servicio.

Es importante señalar que deberán identificarse claramente los objetivos y necesidades de seguridad y resistencia de una organización (p. ej., disponibilidad total de servicios = 99,9 %) basándose en criterios

cuantificables (como, p. ej., la disponibilidad total cada mes), definidos en un acuerdo de nivel de servicio y supervisados continuamente.

Una parte fundamental del proceso de toma de decisiones es llevar a cabo una evaluación comparativa de riesgos (al menos, un análisis DAFO) para obtener una decisión firme y fundada que tenga en cuenta la seguridad de la información y la resistencia desde el momento de la fase de planificación de un proyecto.

Las organizaciones, en su planteamiento respecto a la provisión del servicio, emplearán, finalmente, un modelo de toma de decisiones similar al que se describe en la siguiente figura.

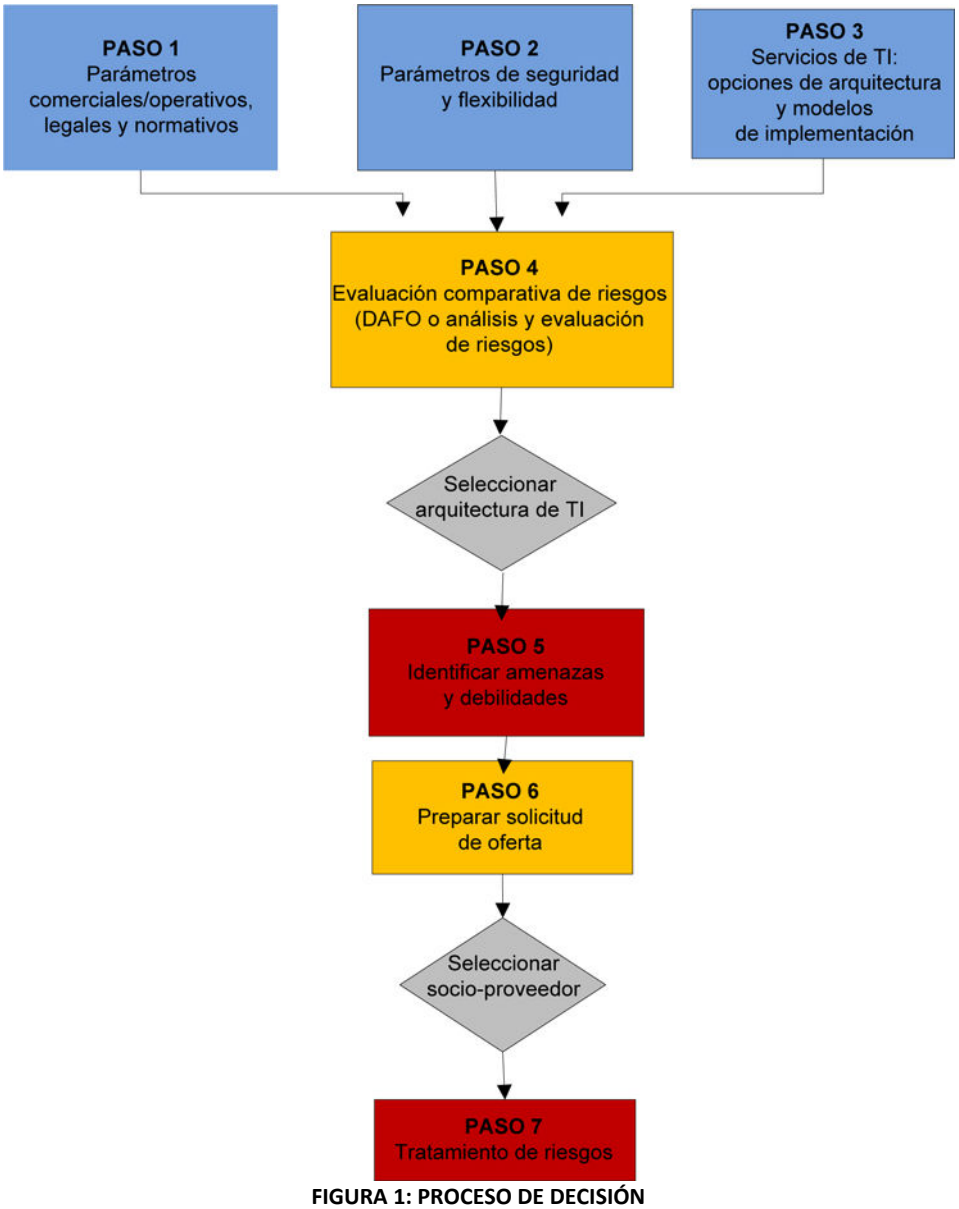


FIGURA 1: PROCESO DE DECISIÓN

En la Figura 1 se muestra el modo en que los requisitos de funcionamiento, jurídicos y de seguridad de la información, así como las limitaciones presupuestarias y temporales, son la guía para la identificación de aquella solución de arquitectura que mejor se adapte a las necesidades de una administración pública, agencia o autoridad sanitaria (pasos 1, 2 y 3).

Por solución de arquitectura, en este informe, nos referimos, a alguna de estas tres opciones: 1) nube pública, 2) nube privada o 3) nube comunitaria. Cada solución puede respaldar uno de los modelos de servicios: IaaS, PaaS o SaaS. La solución de arquitectura híbrida no se ha tenido en cuenta, ya que supone, desde nuestro punto de vista, un segundo paso en el planteamiento respecto a la nube,

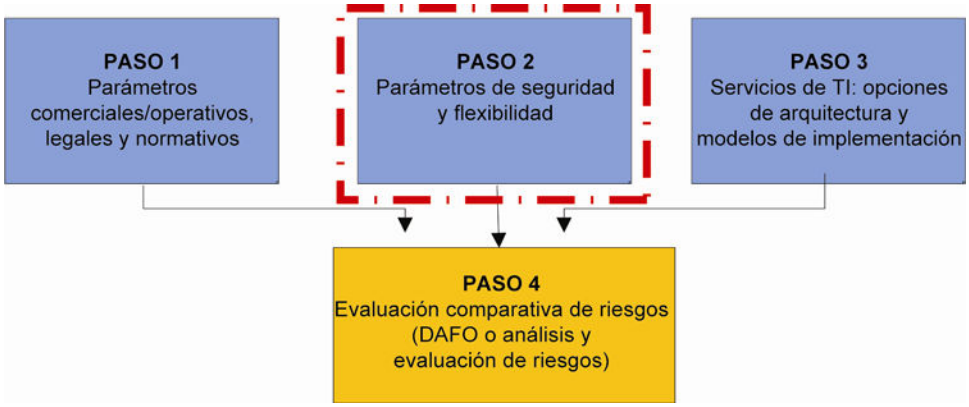
puesto que combina el uso de distintos modelos de nube. La solución de arquitectura híbrida como tal, por tanto, no es objeto de análisis, en ningún sentido, ni positivo, ni negativo. Dicho lo cual, consideramos la distinción entre nube pública, privada y comunitaria el criterio clave para identificar y derivar límites inferiores en relación con los diferentes aspectos de seguridad. En la segunda fase de diseño de arquitectura, corresponde adoptar un planteamiento híbrido al tiempo que se respeta el resultado del análisis anterior.

El modelo más apropiado, en lo que atañe a la seguridad y resistencia, se identifica mediante la realización de una evaluación comparativa basada en criterios específicos de seguridad y resistencia que se derivan, directa o indirectamente, de los requisitos esenciales de un servicio (paso 4). Asumiendo que la evaluación de riesgos del paso 4 confirme que puede considerarse una solución de computación en la nube y, una vez identificada la solución de arquitectura, los siguientes pasos serían: identificar las amenazas y puntos débiles específicos del modelo de servicio de TI seleccionado (paso 5), y la elaboración de una solicitud de oferta para seleccionar un socio comercial, proveedor de servicio o producto (paso 6). Un criterio seguro y prudente respecto a este paso de selección sería identificar una lista de control que se usaría para comparar y evaluar los servicios y soluciones propuestos.

1.5. Parámetros de seguridad y resistencia

En este apartado ofrecemos algunas posibles variables que podrán tenerse en cuenta para comprender los requisitos de un servicio dado.

Como ya se ha mencionado anteriormente en este informe, aparece en primer lugar el paso 2 debido a que la seguridad de la información y la resistencia son los asuntos centrales de nuestro análisis.



En el subapartado 3.1.2, los responsables de la toma de decisiones pueden ver un conjunto de variables de seguridad y resistencia que, probablemente, deban tenerse en cuenta al definir sus requisitos.

Servicio de extremo a extremo seguro y fiable

> *Resistencia* (*resilience*) es la capacidad de un sistema (red, servicio, infraestructura, etc.) de ofrecer y mantener un nivel de servicio aceptable frente a diversos fallos y desafíos al funcionamiento normal.
>
> *Seguridad* es la capacidad de *proteger la información y sistemas de información frente a accesos, uso, divulgaciones, interrupciones, modificaciones o destrucciones no autorizados, así como de responder y recuperarse en caso de fallo o incidencia* (12).

En este informe asumimos que la seguridad de los datos y la resistencia del servicio se tienen en cuenta a la hora de definir el nivel aceptable de servicio para cada organización. De ahí que un servicio pueda considerarse de extremo a extremo seguro y fiable cuando su desempeño se corresponda con lo descrito en la especificación del nivel de servicio.

En el contexto de este estudio, esto supone que un servicio debe ofrecer:

- Un nivel de confidencialidad, integridad y disponibilidad de los datos acorde con los requisitos especificados.
- Un nivel de disponibilidad y fiabilidad del servicio acorde con los requisitos especificados.
- Cumplimiento de la legislación vigente aplicable.

La ausencia de uno o de más de los citados requisitos acarreará la no idoneidad del servicio para cumplir los requisitos de nivel de servicio y satisfacer las expectativas de los usuarios.

Al considerar los aspectos técnicos de la seguridad y resistencia de extremo a extremo será preciso tener en cuenta la organización de los componentes de la arquitectura de toda la cadena de suministro: clientes, red (como LAN, WAN), centros de datos, servicios públicos, gestión de sistemas y servicios de seguridad, así como las soluciones adoptadas a nivel de infraestructura, plataforma, aplicación y datos.

En otras palabras, cada organización deberá considerar de qué modo se podría crear la cadena de suministro de prestación de servicios en su conjunto a partir de una combinación de infraestructura interna y servicios proporcionados por proveedores externos. Por tanto, es necesario prestar atención a todos los componentes y a sus interconexiones a lo largo de la cadena de suministro, como las comunicaciones entre el cliente usuario y la aplicación, entre la aplicación y la base de datos, entre redes (LAN a LAN, LAN a WAN, etc.), así como los componentes de hardware, chips, etc.

El cumplimiento de la legalidad es un requisito que tiene la misma importancia que los requisitos técnicos y de organización sobre seguridad y resistencia. De hecho, de no concurrir, suscitaría controversias jurídicas con particulares, o entre administraciones y gobiernos locales o regionales, conflictos y controversias con las autoridades reguladoras nacionales respecto a la protección de telecomunicaciones y datos, así como con los organismos que velan por el cumplimiento de la legislación. Por último, podría impedir a las administraciones públicas ofrecer sus servicios.

Parámetros de selección de seguridad y resistencia

En este subapartado, sugerimos, basándonos en el informe de ENISA *Metrics for resilience*[7], un conjunto de parámetros de seguridad y resistencia que deben tenerse en cuenta a la hora de evaluar la posible implementación y provisión de modelos de servicios de TI.

Presentamos algunas consideraciones que las agencias gubernamentales y organizaciones de las administraciones públicas que evalúen los servicios de la nube deben tener en cuenta al definir sus requisitos de servicio.

Estos parámetros cualitativos y cuantitativos que proponemos se basan, sobre todo, en el informe de ENISA *Metrics for resilience*. Hemos agrupado conjuntos de parámetros en cuatro categorías que describen la mayor parte de los requisitos que deberán considerarse al planificar un servicio de extremo a extremo seguro y fiable. Las cuatro categorías son:

1. Preparación: incluidos los parámetros y criterios empleados para entender el nivel de preparación de una organización para mantener eficazmente un nivel de servicio aceptable a la vez que se protege la confidencialidad e integridad de los datos tanto durante las operaciones diarias como en caso de tener lugar alguna incidencia.

2. Prestación de servicios: incluidos los criterios empleados para evaluar la capacidad de los sistemas para ofrecer un nivel de servicio en línea con los requisitos expresados en el acuerdo de nivel de servicio.

3. Respuesta y recuperación: incluidos los criterios de medición de la capacidad del sistema para reaccionar en casos de incidencias o fallos.

4. Cumplimiento de la legalidad y la normativa: incluidos los criterios de evaluación del nivel de cumplimiento de la legalidad.

La mayor parte de los parámetros sugeridos son, o pueden ser, criterios y parámetros de supervisión de la ejecución segura de las operaciones en la nube, así como criterios para comprender si se cumplen o no los acuerdos de nivel de servicio.

Cabe destacar que la gobernanza del nivel de seguridad en cada organización afectará a la forma en la que puedan aplicarse los controles subyacentes a los parámetros sugeridos y que, por tanto, va a influir en gran medida en la seguridad y resistencia del servicio en sí. A mayor nivel de gobernanza, mayor grado de control sobre los parámetros sugeridos a continuación.

Afirmamos, en términos generales, que el modelo de servicio SaaS es, claramente, la solución que ofrece al cliente el menor grado de control directo sobre los parámetros de seguridad y resistencia, y que otorga un mayor grado de control y responsabilidad a los proveedores de los servicios de la nube;

[7] http://www.enisa.europa.eu/act/res/other-areas/metrics

por su parte, el IaaS es el que garantiza más capacidad de control directo, pero, al mismo tiempo, deja al cliente con toda la responsabilidad de implementar las medidas técnicas y procedimentales de seguridad y resistencia (véase *Division of Responsibilities* en el informe de ENISA de 2009).

Los siguientes apartados presentan algunos parámetros seleccionados que deberán entender las organizaciones al desarrollar los requisitos para la migración al servicio de la nube. Todas las partes de la solución de extremo a extremo deberán abordar dichos requisitos, incluida la propia organización, los proveedores de la nube y los de la red y las telecomunicaciones que participen en la prestación del servicio.

A. Preparación

Estos parámetros describen el nivel de preparación que se exige a un sistema para continuar frente a fallos e incidencias. Los parámetros relativos a la preparación incluyen todas aquellas acciones y medidas emprendidas para evitar que se produzcan incidencias o bien para reducir el impacto de las mismas.

A1. Análisis y evaluación de riesgos

En este apartado sugerimos una serie de criterios que abarcan la idoneidad de las prácticas de análisis e evaluación de riesgos.

- Frecuencia del análisis y evaluación de riesgos.
- Cobertura de la evaluación de la vulnerabilidad.
- Frecuencia de evaluación de la vulnerabilidad.
- Frecuencia del test de seguridad (p. ej., los test de penetración).

Se puede afirmar, como consideración general, que las nubes privadas deben ofrecer un mayor grado de personalización de las prácticas de análisis y evaluación de riesgos, de modo que una administración pública pueda definir más fácilmente la frecuencia y cobertura de los test y los análisis de acuerdo con sus requisitos particulares.

A2. Prevención y detección

En esta parte incluimos parámetros que miden el grado en el que un organismo público requiere que se supervise el servicio en tiempo real, así como si los mecanismos de limitación de recursos vigentes resultan adecuados para garantizar una utilización de los recursos que sea susceptible de ser controlada.

En la categoría de supervisión de la seguridad en tiempo real, incluimos la integridad y el rendimiento de la red y del sistema operativo, la comparación de referencia y los intentos de acceso no autorizados, además de la supervisión de la seguridad (recopilación, análisis y selección de todo aquello que guarde relación con la seguridad que se hubiese generado desde los cortafuegos, los

sistemas de prevención y detección de intrusos, *proxies*, antivirus, cortafuegos de aplicaciones y cualquier otro componente de la red y la seguridad).

- Frecuencia de los informes.
- Mecanismos de limitación de recursos vigentes.

A3. Administración de parches

Proponemos el empleo de las siguientes medidas para verificar la eficacia de la administración de parches.

- Tiempo medio para el parche.
- Cobertura de la administración de parches.

A4. Control de acceso y exigencia de responsabilidad

Los parámetros que se incluyen en este apartado dan prioridad a la recopilación de pruebas (registros) que demuestren la solidez de los procesos y mecanismos vigentes de control de la autenticación, autorización y rendición de cuentas (*accountability*) de los usuarios.

- Nivel de disponibilidad de los registros.
- Visibilidad de los registros.

A5. Cadena de suministro

Cuanto mayor sea el control mantenido sobre la cadena de suministro de la prestación de servicios, mayor grado de seguridad y resistencia se logrará. Si se tiene esto presente, sugerimos un parámetro de *auditabilidad* como vía para entender el posible nivel de transparencia y control de la cadena de suministro; más concretamente:

- El tipo de auditoría que puede realizarse (interna, por un tercero independiente, autoevaluación, etc.).
- El ámbito de la auditoría (qué enlaces de la cadena pueden auditarse), metodología usada, etc.

B. Prestación de servicios

Este conjunto de parámetros se incluye con el fin de evaluar los requisitos para que la arquitectura de servicios mantenga un nivel aceptable de servicio frente a imprevistos, fallos aleatorios, degradaciones del desempeño o ataques premeditados. En las nubes públicas o comunitarias, algunos de los problemas mencionados podrían surgir debido a los usuarios que comparten la nube. Por tanto, tales problemas podrían resultar críticos cuando una organización no pueda controlar la plataforma o infraestructura. En el caso del SaaS, los parámetros de la prestación de servicios dependen

completamente de la arquitectura de software interna controlada por el proveedor. En los casos de los servicios IaaS y PaaS, se permite un mayor grado de control sobre estos parámetros; aunque debe quedar claro que es necesario un alto nivel de conocimiento especializado para poder usar adecuadamente estos parámetros de control.

B1. Disponibilidad y fiabilidad

En el caso de los servicios IaaS y PaaS, es posible diseñar e implementar el sistema en su conjunto con el fin de obtener mejores valores en relación con la tolerancia a fallos y a ataques maliciosos. Al mismo tiempo, la disponibilidad de un servicio en la nube dependerá muchas veces de la red que se emplee para acceder; por lo tanto, algunas de las medidas se aplicarán también a los proveedores de servicios de Internet. Los parámetros que deberán emplearse para determinar la disponibilidad y fiabilidad de los servicios son:

- Tiempo medio hasta que se produce un fallo.
- Tiempo medio entre fallos
- Disponibilidad total mensual (o diaria).
- Tasa de incidencias.
- Tolerancia a ataques maliciosos.
- Redundancia.
- Replicación.

Otros parámetros que pueden emplearse, en particular, en lo relativo a la integridad de los datos, serían, por ejemplo, los siguientes:

- Porcentaje de sistemas con actualizaciones de definición y de escaneado de virus automáticas.
- Porcentaje de sistemas que efectúan verificaciones de contraseñas de acceso.
- Longitud de las claves de cifrado.
- Uso de controles de integridad y no repudio, p. ej., funciones de suma de control, funciones de *hash* (dispersión), huellas dactilares y funciones de *hash* criptográfico.

Además, el tiempo de respuesta al usuario se ve afectado por la calidad de las conexiones de red entre el usuario y la nube, además de las que haya en el interior de la propia nube. Incluso en el caso de que la nube estuviese adecuadamente diseñada e implementada, en caso de que la conexión a la nube fuese lenta, el desempeño de la nube para los usuarios se vería afectado negativamente. Los parámetros más importantes incluyen los siguientes:

- Rendimiento (ancho de banda).

- Latencia (tiempo medio de ida y vuelta (*round trip*)).
- Pérdida de paquete.
- *Jitter* (variación de demora de paquete).

Teniendo en cuenta que la disponibilidad y la fiabilidad son dos de los parámetros esenciales de la evaluación de la resistencia del servicio, es de vital importancia que las medidas y criterios que se empleen guarden coherencia y que el objeto de la medición sea el mismo en todo caso. En este informe, nos referimos en todo momento a la disponibilidad y fiabilidad del servicio para los usuarios finales.

B2. Escalabilidad y elasticidad

La *gestión de capacidad* es el proceso responsable de asegurar que la capacidad de los servicios e infraestructuras de TI es capaz de prestar el nivel de servicio objetivo acordado de forma rentable y en el tiempo adecuado. La gestión de capacidad tiene en cuenta todos los recursos necesarios para prestar el servicio de TI y planifica los requisitos de negocio a corto, medio y largo plazo (13).
La capacidad de gestionar los cambios en los recursos demandados (almacenamiento, tiempo de la CPU, memoria, solicitudes de servicio web e instancias de máquinas virtuales, etc.) y de escalabilidad, en ambos sentidos, supone un factor crucial para la eficacia del servicio. Así pues, al considerar la gestión de la capacidad y la demanda, será preciso tener en cuenta dos criterios importantes; a saber:

- Las fluctuaciones de capacidad: la impredecible de las variaciones de carga de tráfico, las fluctuaciones de capacidad de enlace, fallos de nodos u otros tipos de incidencias provocadas que podrían causar sobrecargas de la red.
- La escalabilidad (en ambos sentidos) a largo plazo: la capacidad del sistema de aumentar o reducir su capacidad para ofrecer los recursos solicitados en un tiempo adecuado para poder cumplir los requisitos de nivel de servicio.

Los siguientes parámetros se refieren a la capacidad de una aplicación de explotar completamente todos los recursos que ofrece la nube para reaccionar a los cambios de carga que se imponen en una aplicación. Los parámetros más importantes incluyen los siguientes:

- Tolerancia de carga: puede calcularse como el ratio de la carga máxima que puede soportar un sistema en comparación con la carga normal esperada, p. ej., el porcentaje de la carga normal que puede escalar un sistema temporalmente (anchura de banda, capacidad de procesamiento, etc.). La unidad es relativa; indica la variación permitida en la carga del sistema sin que afecte al rendimiento en su conjunto. Debe señalarse, asimismo, que la tolerancia de carga para dos proveedores de servicio de igual tamaño con el mismo ratio carga máxima-carga normal puede derivar en distintos niveles de tolerancia en el caso de que uno de ellos sirviese a miles de pequeños clientes y, el otro, solo a unos pocos muy grandes.

- Tolerancia de tráfico (incluidas provisiones anti-DoS/DDoS, p. ej., filtrado, cortafuegos, re-enrutamiento, suspender el servicio a clientes que produzcan tráfico excesivo, etc.): La capacidad de un sistema de tolerar cargas impredecibles sin una caída importante en la carga soportada (incluido el colapso de congestión), así como de aislar los efectos del tráfico cruzado, otros flujos y otros nodos. El tráfico puede ser inesperado pero legítimo, como un *flash crowd*, o malicioso, como un ataque DDoS.
- La variabilidad de carga de los servicios (la diferencia entre demanda pico y demanda media).

Otros parámetros que hay que considerar son los relacionados con la provisión de los servicios y componentes de hardware, por ejemplo:

- Tiempo para obtener nuevos componentes de hardware.
- Tiempo de cumplimiento del servicio (implementación y provisión del servicio).

Cabe destacar que dichos parámetros son de especial importancia cuando se compara el modelo de computación en la nube con una solución de TI convencional.

C. Respuesta y recuperación:

Estos parámetros se refieren a la capacidad de una organización de responder adecuadamente y recuperarse de forma eficaz de las incidencias. Deberán identificarse el RTO (objetivo de tiempo de recuperación, cuánto tiempo) y el RPO (objetivo de punto de recuperación) necesarios. En esta fase, una organización tendrá que considerar el momento en el que es necesario activar el plan de resistencia; a quién debe informarse y los canales que deben emplearse. La organización debe asegurarse de que cuenta con la capacidad (equipo de analistas) de comprender a tiempo las raíces que ocasionan la incidencia y su impacto (comprender lo sucedido). La organización debe asegurarse de que se rastrea la incidencia durante el ciclo vital de ésta (lección identificada), y que el suceso se comunica de forma adecuada al mundo externo. Por último, es preciso probar los planes de respuesta y recuperación.

Con el fin de medir la eficacia y eficiencia de la estrategia de respuesta y recuperación que se aplica, deberán emplearse los siguientes criterios:

- Tiempo medio de descubrimiento de la incidencia (demora): el tiempo que lleva descubrir la incidencia desde el momento en que tiene lugar.
- Tiempo para la activación: el tiempo que lleva darse cuenta de que la fase de recuperación-respuesta debe activarse (tiempo medio para la activación).
- Tiempo para reparar (tiempo medio para reparar): el tiempo que lleva recuperar el servicio dentro de un nivel aceptable.

- Tiempo medio de recuperación de la incidencia.

Debe destacarse que existe una relación entre algunos de los parámetros, como el tiempo de recuperación y la frecuencia y arquitectura de los sistemas de *backup* usados.

D. Cumplimiento de la legalidad y la normativa:

Estos parámetros se refieren, en general, a los requisitos del acuerdo de nivel de servicio del proveedor de servicios de la nube y a las disposiciones contractuales (estados de ejecución del sistema, p. ej.).

D1. Informática forense

- Requisitos de la extracción de pruebas contenidas en los servicios de la nube (p. ej., obtención de datos para fines judiciales (*e-discovery*), retención de datos).

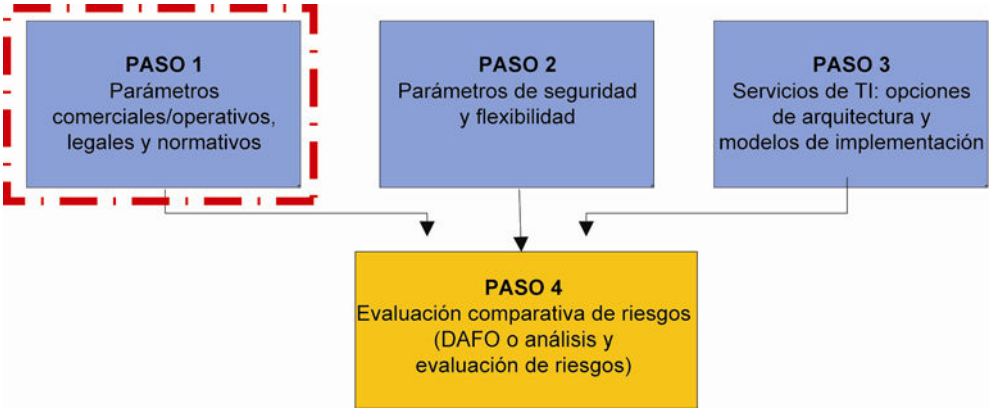
D2. Retención de datos y trazabilidad (*track back*)

- Periodos mínimo y máximo de retención de datos.
- Periodos mínimo y máximo de retención de registros.
- Modalidad de almacenamiento de los datos.
- Modalidad de almacenamiento del registro.
- Tiempo de transferencia al origen.

D3. Confidencialidad

El grado de confidencialidad necesario dependerá de la legislación nacional de cada país, es decir, sanidad pública, datos de la seguridad social y datos fiscales. Las posibles implicaciones de este requisito son las soluciones de cifrado que se le exijan al proveedor, p. ej., la longitud de la clave.

3.2. Variables de negocio y operativas



En este apartado se sugieren una serie de criterios que probablemente deban ser considerados cuando se definan los requisitos de negocio, operativos, legales y reglamentarios para las organizaciones públicas.

Algunos de los criterios y parámetros sugeridos se explican y describen, mientras que otros solo se enuncian.

Tipos de datos

Uno de los criterios más importantes a tener en cuenta, al considerar la implementación de una solución en la nube, es el tipo de datos que el proveedor de servicios procesará y almacenará.

De acuerdo con lo que se menciona en las tres situaciones hipotéticas que se presentan en este informe, los tipos de datos a considerar son:

- **Datos personales**: nombres, domicilios, ocupaciones, detalles de contacto, etc.
- **Datos sensibles**: propiedad intelectual, datos confidenciales y de transacciones financieras de empresas e historias clínicas.
- **Información clasificada**.
- **Datos agregados**: la información que se puede inferir a partir de los datos que han sido agregados, al permitir la inferencia de información o simplemente almacenando conjuntamente datos que no deberían estar relacionados debido a su sensibilidad. Téngase en cuenta que las agregaciones de datos son consideradas bajo la Directiva de protección de datos de la UE como el estudio y la consideración de los datos.

Perfil de usuario

El análisis del perfil de usuario representa un criterio muy importante a tomar en consideración, especialmente en nubes comunitarias y privadas (por ejemplo, ver la situación hipotética "Nube gubernamental como vivero de empresas"). Dependiendo del tipo de usuarios potenciales y su

distribución geográfica, se identificarán los otros requisitos de negocio y se diseñarán las características técnicas.
En principio, tres importantes características a considerar son:

- Comunidades de usuarios (ciudadanos, empresas y otras administraciones públicas).
- Distribución geográfica.
- Nivel de formación en TIC y conciencia sobre la seguridad.

Escalabilidad y gestión de capacidad

La *gestión de capacidad* es el proceso responsable de asegurar que la capacidad de los servicios e infraestructuras de TI es capaz de prestar el nivel de servicio objetivo acordado de forma rentable y en el tiempo adecuado. La gestión de capacidad tiene en cuenta todos los recursos necesarios para prestar el servicio de TI y planifica los requisitos de negocio a corto, medio y largo plazo (13).
La capacidad de gestionar los cambios en los recursos demandados (almacenamiento, tiempo de la CPU, memoria, solicitudes de servicio web e instancias de máquinas virtuales, etc.) y de escalabilidad, en ambos sentidos, supone un factor crucial para la eficacia del servicio. Así pues, al considerar la gestión de la capacidad y la demanda, será preciso tener en cuenta dos criterios importantes; a saber:

- Las fluctuaciones de capacidad: lo impredecible de las variaciones de carga de tráficos, las fluctuaciones de capacidad de enlace, fallos de nodos u otros tipos de incidencias provocadas que podrían causar sobrecargas de la red.
- La escalabilidad (en ambos sentidos) a largo plazo: la capacidad del sistema de aumentar o reducir su capacidad para ofrecer los recursos solicitados en un tiempo adecuado para poder cumplir los requisitos de nivel de servicio.

Interoperabilidad de interfaz

La interoperabilidad es la habilidad de dos o más sistemas o componentes para intercambiar información y utilizar la información que se ha intercambiado (14).

En este estudio se consideran los siguientes atributos para describir las necesidades de interoperabilidad de los servicios:

- Interoperabilidad de interfaz / complejidad de interfaz.
- Capacidades de intercambio del formato de datos.
- Métodos de transferencia / intercambio.
- Sistema de identidad.
- Interoperabilidad de políticas.

Colaboración

La colaboración entre sistemas, plataformas y servicios debe tener en cuenta:

- La dispersión geográfica de las entidades (organizaciones, infraestructuras).

- Los demás requisitos del servicio.
- El nivel de heterogeneidad de los sistemas TIC implicados.

Costo y presupuesto

A pesar de que las implicaciones presupuestarias y financieras no se encuentran dentro de los objetivos de este informe, nos gustaría poner de relieve los factores básicos que los directores generales, directores de tecnología y directores de seguridad suelen tener en cuenta a la hora de evaluar las inversiones en TIC, puesto que un uso racional del presupuesto disponible tiene un impacto en la cantidad de recursos que pueden dedicarse a la seguridad de la información.

A tal efecto, las tres variables más importantes a tener en cuenta son:

- Los costes operativos.
- El gasto de capital.
- El coste de migración.

Propiedad

- Propiedad gubernamental prestada por las propias administraciones públicas.
- Propiedad gubernamental, operada por un tercero.
- Patrocinado por las administraciones públicas.
- Proporcionado por un tercero, definido por las administraciones públicas.
- Asociación.
- Código de la conexión o una declaración de cumplimiento.

3.3. Marco legal y regulador

Consideraciones legales generales

A medida que el estado de derecho se aplica a los actores gubernamentales en todos los Estados Miembros, éstos están directamente obligados por sus respectivas constituciones. Este hecho está en franco contraste con los actores privados que disfrutan de plena autonomía privada ("liberalismo") a menos que existan leyes que limiten sus acciones. A veces esto no resulta muy evidente, sobre todo porque muchas leyes (sub-constitucionales) se aplican a los actores gubernamentales y garantizan el cumplimento de los requisitos constitucionales. En ocasiones estas leyes se aplican incluso de manera similar en las administraciones públicas y en el sector privado. Así, en la mayoría de los casos, la discusión de esta legislación subconstitucional será totalmente suficiente a los efectos de este análisis.

Soberanía y control gubernamentales sobre la información y los datos: cuestiones sobre el acceso a la aplicación de la ley, la confidencialidad y la propiedad intelectual

Para los gobiernos y las administraciones públicas en general, una de las principales cuestiones jurídicas es la soberanía y el control sobre los datos que se están manejando. Un organismo gubernamental que tiene derecho a manejar datos tiene la responsabilidad de realizar un uso adecuado de éstos y de garantizar que sus obligaciones de proteger los datos se extienden por contrato a sus proveedores terceros. Cuando el alojamiento de infraestructuras de la nube se extienda más allá de la jurisdicción local, el organismo público debe tener en cuenta las implicaciones y garantías correspondientes ofrecidas por su proveedor o proveedores. Si los datos gubernamentales están siendo utilizados fuera por grupos privados en jurisdicciones extranjeras, esto crea el riesgo de que los tribunales extranjeros citen a comparecer a la entidad privada y, por lo tanto, tengan acceso a los datos del gobierno. Además, esto puede significar violaciones potenciales de las leyes de confidencialidad y de propiedad intelectual relacionadas con la información, datos, *know-how*, *copyright* o patentes transferidos a la nube.[8] Estas cuestiones se aplican por igual a todas las formas de contratación externa, incluido cualquier acuerdo actual de contratación externa, así como la provisión de nubes públicas, privadas y comunitarias. Por lo tanto, un organismo gubernamental deberá garantizar que sus proveedores de externalización imponen las medidas de seguridad adecuadas, y que existen los procedimientos y mecanismos para asegurar que solo se entregarán los datos relevantes en respuesta a demandas legítimas de las autoridades judiciales. Esto incluye la comprobación de si las pruebas se han solicitado legítimamente (por una citación judicial o durante una búsqueda de datos (*discovery*)).[9]

Contratación pública

Debido a que se suele contratar a entidades privadas para prestar servicios en la nube, se deberá observar la amplia normativa de la UE en materia de contratación pública.[10] En este sentido, no habrá ninguna diferencia significativa respecto a la contratación que se realice en otras áreas de las administraciones públicas, por lo que los gobiernos y administraciones públicas podrán aplicar sus conocimientos y experiencias junto con las leyes y reglamentos aplicables. Por otro lado, los proveedores de servicios en la nube deben cumplir los requisitos de precalificación como proveedores de acuerdo con las regulaciones de la UE sobre contratación pública y, por lo tanto, ajustarse a los reglamentos relativos a la contratación pública.

Protección de datos y seguridad de los datos

Los temas relacionados con la protección y la seguridad general de datos en Europa relacionados con la computación en la nube ya se han señalado en: (i) recientes comunicaciones de la Comisión Europea; (ii) los textos adoptados por el Grupo de Trabajo establecido en virtud del artículo 29; y (iii) el informe de ENISA: "Cloud Computing Risk Assessment" ("Evaluación de los riesgos de la computación en la nube") (15).

---

[8] *Para más información sobre cuestiones relacionadas con la confidencialidad y la propiedad intelectual, consulte el documento de ENISA de 2009 titulado "Cloud Computing Risk Assessment" ("Evaluación de los riesgos de la computación en la nube"), pág. 97 y siguientes.*

[9] *http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp158_en.pdf*

[10] *Véase: http://ec.europa.eu/internal_market/publicprocurement/legislation_en.htm*

Aquí vamos a tratar de resumir los más relevantes para el presente análisis.

- *Restricción a la aplicabilidad de la Directiva 95/46/CE (Artículo 13(1)):*

  De conformidad con el Artículo 13(1) de la Directiva 95/46/CE, los Estados miembros podrán limitar la aplicación de determinadas disposiciones de la Directiva 95/46/CE en materia de seguridad nacional y pública o el enjuiciamiento y la prevención del crimen.[11] Así, en función de la legislación local en un Estado miembro, en determinadas circunstancias algunos datos que manejen los municipios pueden no estar sujetos a todas las normas establecidas en la Directiva 95/46/CE.

- *Responsable del tratamiento de datos – Encargado del tratamiento de datos (Directiva 95/46/CE, Artículos 2(d) y (e)):*

  Se debe identificar al responsable del tratamiento, el encargado del tratamiento y sus interacciones con el fin de determinar "quién es el responsable del cumplimiento de las normas de protección de datos, cómo pueden ejercer los interesados sus derechos, cuál es la legislación nacional aplicable y cuál es la eficacia con la que las Autoridades de Protección de Datos pueden operar" (16)[12]. La Directiva 95/46/CE distingue claramente entre el responsable del tratamiento (*controller*) y el encargado del tratamiento (*processor*). El *responsable del tratamiento* es la persona o entidad que determina los fines y los medios para el tratamiento de los datos personales. El *encargado del tratamiento* es la persona o entidad que procesa datos personales por cuenta del responsable del tratamiento. Sin embargo, la aplicación de esta definición al entorno de la computación en la nube es todo un reto. A primera vista, uno podría concluir que las administraciones públicas/gobierno es el responsable del tratamiento y que el proveedor de servicios en la nube es el encargado del tratamiento.[13] Sin embargo, los proveedores de servicios en la nube suelen determinar los medios y, a veces también, los fines del tratamiento, por lo que entran dentro de la definición de responsable del tratamiento (17). Para solucionar este problema y ofrecer algunas orientaciones sobre el Artículo 29, el Grupo de Trabajo sobre Protección de Datos emitió un dictamen el 16 de febrero de 2010 en el que aprobó un punto de vista sobre la interpretación de tales definiciones en entornos complejos. (16). Sin embargo, el dictamen no arrojó mucha luz sobre los detalles específicos del entorno de computación en la nube, para el cual aún deben determinarse los papeles de responsable del tratamiento y encargado del tratamiento caso por caso y en relación con la naturaleza de los servicios en la nube[14] (18)

---

[11] *Se permiten restricciones con respecto a las obligaciones y derechos previstos en los Artículos 6(1) (principios relativos a la calidad de los datos), 10 y 11(1) (información que debe suministrarse al interesado), 12 (derecho de acceso) y 21 (publicidad de las operaciones de procesamiento).*

[12] *Grupo de Trabajo del Artículo 29: Dictamen 1/2010 sobre los conceptos de responsable del tratamiento y encargado del tratamiento.*

[13] *ENISA (2009), Cloud Computing Risk Assessment ("Evaluación de los riesgos de la computación en la nube"), pág. 101 y sig.*

[14] *El supervisor europeo sobre protección de datos, Peter Hustinx, confirmó este enfoque en su discurso sobre 'Protección de datos y Computación en la nube bajo la legislación de la UE' impartido el 13 de abril del 2010, donde hizo un llamamiento*

- *Control previo (Directiva 95/46/CE, Artículo 20):*

  De conformidad con el Artículo 20 y en función de la legislación nacional, el control previo puede ser necesario para el tratamiento. Esto depende del tipo de servicio y de los tipos de datos que se procesen.

- *Medidas técnicas y organizativas adecuadas (Artículo 17): integridad de los datos, gestión de identidades y control de acceso*

  La integridad y la disponibilidad de los datos son elementos esenciales en la prestación de los servicios de computación en la nube. De acuerdo con la Directiva 95/46/CE, el responsable del tratamiento y sus encargados deben implementar medidas técnicas y organizativas para proteger los datos personales contra su destrucción accidental o ilícita o su pérdida accidental, alteración, divulgación o acceso no autorizado; teniendo en cuenta el estado de la técnica y el coste de su implementación, dichas medidas deben garantizar un nivel de seguridad adecuado en relación con los riesgos representados por el tratamiento y la naturaleza de los datos a proteger (artículo 17). El problema es que el concepto de "adecuado" se ha interpretado de diferentes maneras en los diferentes Estados miembros de la UE. Así, aunque los proveedores de servicios en la nube aplican muy a menudo normas técnicas reconocidas (por ejemplo, ISO 27001) para asegurar los datos de los clientes, éstas pueden no ajustarse perfectamente a los requisitos nacionales con respecto a las medidas que es adecuado adoptar. Es necesaria una mayor coherencia y armonización en la UE. Además, vale la pena tener en cuenta el elevado nivel de seguridad de los datos solicitado a un proveedor de servicios en la nube en un contexto de sanidad electrónica, con especial atención a la gestión de identidades y el control de acceso.

- *Filtración de datos y notificación de incidentes de seguridad (no obligatorio, todavía)*

  El marco revisado de la UE para las comunicaciones electrónicas aclara las responsabilidades de los operadores de redes y los proveedores de servicios, incluyendo su obligación de notificar violaciones de la seguridad de los datos personales (artículos 4 y 13). La revisión del marco general de protección de datos emprendida recientemente incluirá una posible extensión de la obligación de notificar las violaciones de seguridad de los datos (19) (8). Si las regulaciones europeas sobre protección de datos van en este dirección, será necesario que se identifique claramente el grado de violación de la seguridad de los datos que se debe notificar, a quién se debe notificar (cliente del proveedor de servicios en la nube, autoridad competente en cuanto a protección de datos, interesados) y las modalidades pertinentes. Una obligación indeterminada de notificar cualquier violación (incluso las menores o insignificantes) de la seguridad de los datos puede perjudicar gravemente a los proveedores de servicios en la nube

para obtener más ayuda del Grupo de Trabajo sobre la materia. La computación en la nube se encuentra en la Agenda del Grupo de Trabajo para los años 2010 y 2011.

y generar una alarma innecesaria de los gobiernos, las administraciones públicas y los ciudadanos en general.

- *Transferencia de datos a países de fuera del Espacio Económico Europeo (Artículos 25-26)*

  Los modelos en la nube suponen que la información y los datos del cliente pueden implicar la transferencia de datos por parte del proveedor de servicios en la nube desde un centro de datos en el Espacio Económico Europeo (EEE) a otro que puede estar ubicado en cualquier parte del mundo. Sin embargo, la Directiva 95/46/CE prohíbe las transferencias de datos personales desde el EEE a países que no garanticen un nivel adecuado de protección en el sentido del artículo 25(2) (a menos que el interesado haya dado previamente su consentimiento inequívoco a la transferencia propuesta o se hayan establecido otros procedimientos de conformidad con el artículo 26 (por ejemplo, "Contratos tipo para la transferencia de datos personales a terceros países", "Principios de puerto seguro" (donde los datos se están transfiriendo a los Estados Unidos) o "Normativas corporativas vinculantes")[15]. Sin embargo, existen problemas con cada uno de estos modos de legitimar una transferencia: el hecho de basarla en el consentimiento del interesado expone la transferencia a las incertidumbres de la posible retirada de dicho consentimiento; los Principios de puerto seguro, que se aplican a los datos transferidos a los Estados Unidos, pueden quedarse cortos en un entorno de nube, donde los flujos de datos pueden referirse a países no pertenecientes al EEE distintos de los Estados Unidos; y las Normativas corporativas vinculantes (NCV) aún no han sido plenamente respaldadas por los proveedores de servicios en la nube principales, debido principalmente a deficiencias en el proceso de aplicación y aprobación de las éstas. Los proveedores en la nube a menudo deben recurrir al uso de contratos tipo para respaldar las transferencias de datos repetitivas o múltiples, pero puede ser costoso poner en práctica dichos contratos, especialmente allí donde las normativas nacionales imponen requisitos administrativos adicionales (tales como el deber de obtener la aprobación reglamentaria del contrato). A la luz de estos retos, y como parte del examen del marco de protección de datos de la UE, la Comisión Europea tiene como objetivo mejorar los mecanismos de transferencia de datos a países que no pertenecen al EEE. La Comisión también está alentando las iniciativas de autorregulación, como los códigos de conducta o los códigos de práctica.[16] No obstante, en el caso de servicios en la nube proporcionados a los gobiernos y administraciones públicas,

---

[15] *La Directiva 95/46/CE permite transferir datos personales fuera del EEE solo cuando el tercer país proporciona un "nivel suficiente de protección" para los datos (artículo 25) o cuando el responsable del tratamiento aduce que existen garantías suficientes respecto a la protección de la privacidad (artículo 26). Las Normas corporativas vinculantes (NCV) son una de las formas en que un grupo de empresas puede demostrar que se cumplen tales garantías suficientes (artículo 26) con respecto a las transferencias internas del grupo, si bien las NCV no son una herramienta que aparezca o se muestre expresamente en la Directiva. Véase el Artículo 29 en los Data Protection Working Party Opinions (dictámenes del Grupo de Trabajo sobre Protección de Datos) 74, 133, 153, 154, y 155; todos disponibles en: <http://ce.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs>.*

[16] *Discurso de Neelie Kroes, Vicepresidenta de la Comisión Europea para la Agenda Digital, sobre Computación en la nube y protección de datos en Les Assises du Numérique conference, Université Paris-Dauphine, el 25 de noviembre de 2010; disponible en: <http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/10/686&format=HTML&aged=0&language=EN&guiLanguage=en>.*

todos los argumentos sobre la soberanía gubernamental presentados anteriormente serán un factor en relación con las transferencias de datos. Por último, cabe destacar también que hay bastantes cuestiones relativas a la transferencia de datos de pacientes, que se detallan en la sección dedicada al contexto de la sanidad electrónica.

- *Derecho del interesado de acceso a los datos (Directiva 95/46/CE, Artículo 12):*

  El responsable del tratamiento tiene la obligación de garantizar al interesado los derechos establecidos en el artículo 12; por ejemplo, a obtener la confirmación de si se están procesando o no datos relativos al interesado, a obtener información sobre los propósitos del tratamiento, las categorías de los datos en cuestión, el receptor o las categorías de los destinatarios a quienes se comunicarán los datos, a corregir, borrar o bloquear los datos procesados de un modo que no sea compatible con las disposiciones de la Directiva, etc. Es muy importante, especialmente cuando el proveedor de servicios en la nube se engloba en la definición de encargado del tratamiento, que el proveedor de servicios en la nube establezca una cooperación muy estrecha con sus clientes (es decir, gobiernos y administraciones públicas) para asegurar que estos últimos, en su calidad de responsables del tratamiento, estén en condiciones de cumplir sus obligaciones respecto a la protección de datos frente a los interesados. Es conveniente precisar los términos de esa cooperación entre las partes en el contrato correspondiente. Surgen cuestiones específicas a este respecto en el contexto de la sanidad electrónica, en el que es un hecho no solo que la Directiva 95/46/CE se ha puesto en marcha de una manera inconsistente, sino también que los derechos de los pacientes están definidos y se implementan de maneras diferentes según las distintas leyes nacionales que se apliquen.

Disposiciones sobre Interoperabilidad / Transferencias al origen / "Cautividad del mercado"

Una solución de la nube debe ser interoperable, permitiendo a los gobiernos y las administraciones públicas migrar a los servicios en la nube de un proveedor de servicios en la nube a otro sin restricciones técnicas o contractuales o costes de cambio sustanciales. Además, la interoperabilidad será una condición necesaria en el contexto de la sanidad electrónica. Por otra parte, en los contratos debe definirse el calendario y las modalidades de las transferencias al origen de información y datos.

Es muy importante que los gobiernos y las administraciones públicas eviten cualquier forma de "cautividad del mercado", ya que cualquier falta de disponibilidad (temporal) y/o ineficiencia de los servicios puede dar lugar a importantes responsabilidades para los gobiernos y las administraciones públicas (se puede pensar en el daño y la responsabilidad que puede ocurrir en el contexto de la sanidad electrónica).

Negligencia profesional del proveedor de servicios en la nube

Al migrar a los servicios en la nube, los gobiernos y las administraciones públicas pasan a depender mucho de la adecuación del desempeño del proveedor de servicios en la nube. Lo más probable es que los fallos o deficiencias del proveedor de servicios en la nube en la prestación de los servicios tengan un impacto muy negativo sobre los servicios que ofrecen los gobiernos y las administraciones públicas

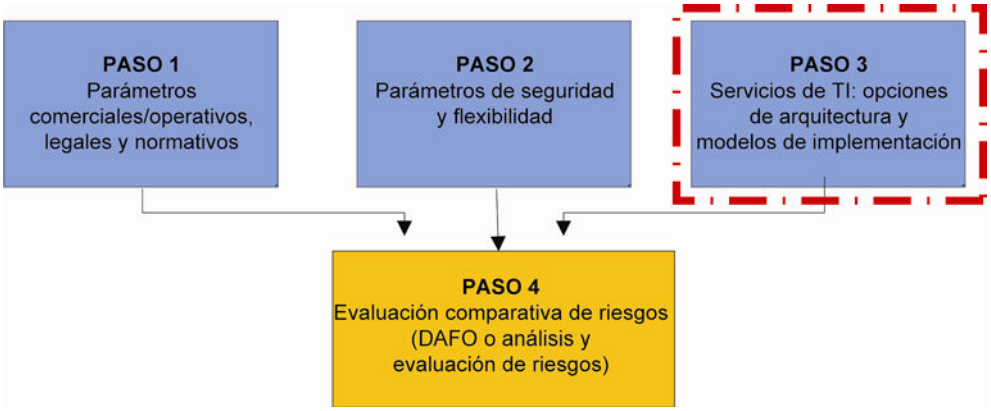
a los ciudadanos. Esto se puede traducir no solo en pérdidas económicas para los gobiernos y las administraciones públicas, sino también en daños a su imagen (por tanto, daño político). Las cláusulas de responsabilidad e indemnización en los acuerdos de nivel de servicio (ANS) van a desempeñar un papel fundamental en este tema. Los ANS detallados, en los que se especifican detalladamente los niveles de funcionamiento del proveedor de servicios en la nube, junto con las cláusulas contractuales que asignan claramente, por un lado, los derechos y deberes generales de las partes y, por el otro, las obligaciones y responsabilidades, serán intereses cruciales de gobiernos y administraciones públicas.

Éstos deberían pedir a los proveedores de servicios en la nube que estén atentos para evitar errores, y asegurar este punto a través de cláusulas contractuales que establezcan sanciones importantes en caso de deficiencias en los servicios del proveedor de servicios en la nube.

La subcontratación de servicios en la nube y el cambio de control del proveedor de servicios en la nube

Dada la relación altamente dependiente, es probable que los gobiernos y las administraciones públicas seleccionen cuidadosamente los proveedores de servicios en la nube. Se deben evitar las situaciones en las que un proveedor de servicios en la nube subcontrate los servicios pertinentes a un tercero o, al menos, se deben incluir en el acuerdo de servicio declaraciones y garantías sobre posibles subcontratistas. Del mismo modo, el proveedor de servicios en la nube debe notificar sin demora los cambios de control al gobierno o administraciones públicas, que es posible que desee negociar el derecho de rescindir el contrato en caso que ocurra tal evento.

3.4. Opciones de arquitectura



En este apartado se han propuesto definiciones cortas para los modelos en la nube.

No nube

- *En propiedad absoluta y completamente gestionada*: los servicios de TI se proporcionan a través de una infraestructura y una plataforma que es de propiedad absoluta y que está gestionada por entero por la misma entidad que utiliza los servicios.

- *Externalizada*: los servicios de TI están subcontratados a un tercero. Los servicios pueden ser proporcionados por una infraestructura o plataforma propiedad de la misma entidad que utiliza los servicios (por ejemplo, un cliente interno) o por una que pertenece al propio proveedor del servicio. La provisión del servicio está regulada por un contrato en el que están claramente definidos los términos, condiciones, sanciones y duración.

Para un descripción más detallada de una opción de arquitectura típica de servicio TI de una no nube, le rogamos que consulte la bibliografía existente (p. ej., ITIL).

Nube

Para las definiciones de los diversos tipos de computación en la nube, normalmente nos referimos al NIST (20).

Modelos de implementación y propiedad

- *Privado*: la infraestructura en la nube es operada exclusivamente por una organización particular. Puede ser gestionada por la propia organización o por un tercero, y puede existir en el mismo inmueble o fuera de él.
- *Público*: la infraestructura de la nube se pone a disposición del público en general o de un gran grupo industrial y es propiedad de una organización que vende servicios en la nube.
- *Comunitario*: la infraestructura de la nube es compartida por varias organizaciones y respalda a una comunidad específica que comparte preocupaciones (p. ej., misión, requisitos de seguridad, política y consideraciones de cumplimiento). Puede ser administrada por las organizaciones o por un tercero y puede existir en el mismo inmueble o fuera de él (20). La 'infraestructura de la nube' podría ser un centro de datos de propiedad exclusiva o una red (federación o comunidad) de centros de datos (más pequeños) (21).

  Para ver un ejemplo de una nube federada o comunitaria, consúltese el Anexo III, Descripción de la Arquitectura del Proyecto Reservoir.
- *Híbrido*: la infraestructura de la nube es una composición de dos o más nubes (privada, comunitaria o pública) que se mantienen como entidades únicas pero que están unidas entre sí por tecnología estandarizada o propietaria que permite la portabilidad de los datos y de la aplicación (p. ej., *cloud bursting* que equilibra la carga soportada por las distintas nubes).

  Una posible configuración de una nube híbrida es representada por una nube privada que escala horizontalmente a una nube pública. Sobre la base de que el modelo híbrido requiere la combinación de dos nubes, se supone que una nube híbrida representa un segundo paso en un enfoque de nube. Teniendo en cuenta el horizonte temporal a corto plazo de este informe, se excluye la nube híbrida de nuestro análisis.

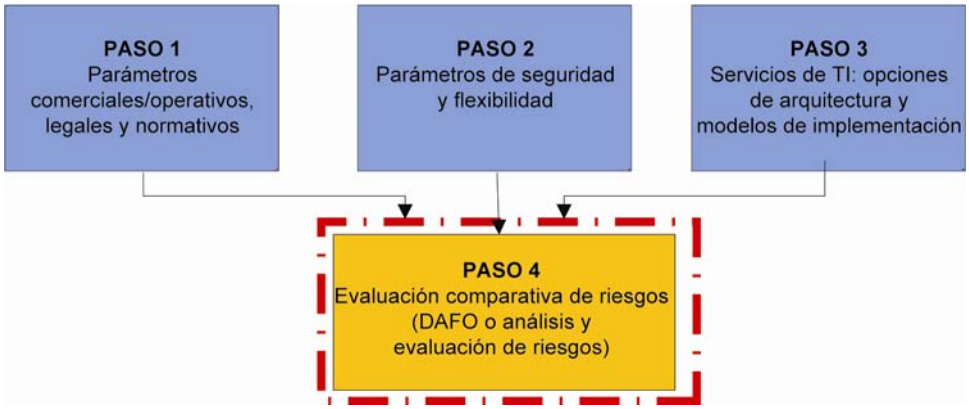
Computación y modelos de prestación

- Software como Servicio (SaaS): la capacidad ofrecida al consumidor es usar las aplicaciones del proveedor ejecutándolas en una infraestructura en la nube. Las aplicaciones son accesibles desde varios dispositivos del cliente a través de una interfaz cliente ligera, como un navegador

web (p. ej., correo electrónico basado en web). El consumidor no gestiona ni controla la infraestructura subyacente de la nube, lo que abarca la red, servidores, sistemas operativos y almacenamiento, o incluso las capacidades individuales de la aplicación, con la posible excepción de parámetros limitados de configuración de la aplicación específicos del usuario.

- Plataforma como Servicio (PaaS): la capacidad ofrecida al consumidor es desplegar, en la infraestructura de la nube, aplicaciones creadas por el consumidor o adquiridas que han sido creadas utilizando lenguajes de programación y herramientas admitidas por el proveedor. El consumidor no administra ni controla la infraestructura en la nube subyacente, lo cual incluye la red, servidores, sistemas operativos y almacenamiento, pero sí tiene control sobre las aplicaciones desplegadas y, posiblemente, las configuraciones del entorno de *hosting* de la aplicación.
- Infraestructura como Servicio (IaaS): la capacidad ofrecida al consumidor es la disposición de procesamiento, almacenamiento, redes y otros recursos informáticos fundamentales en los que el consumidor puede desplegar y ejecutar software, lo que puede incluir sistemas operativos y aplicaciones. El consumidor no administra ni controla la infraestructura subyacente en la nube, pero posee el control de los sistemas operativos, el almacenamiento y las aplicaciones desplegadas y, posiblemente, control limitado sobre determinados componentes de la red (p. ej., cortafuegos de anfitrión).

Análisis DAFO



En este capítulo se presentan los resultados de una evaluación comparativa de los modelos de implementación de la nube pública, privada y comunitaria basados en los parámetros de seguridad, resistencia y cumplimiento establecidos en el punto 3.1.2.

El análisis identifica los puntos fuertes, los débiles, las oportunidades y las amenazas de cada modelo de nube.

Se utiliza el análisis DAFO como una herramienta para la comparación, pero se podrían utilizar en su lugar métodos más exhaustivos, como una evaluación de riesgos. De hecho, se debe considerar el análisis de puntos fuertes, débiles, oportunidades y amenazas como la acción inicial (y mínima) a llevar a cabo, pero debe llevarse a cabo una evaluación de riesgos más detallada para sustentar una identificación más precisa y una evaluación de los riesgos que afectan a una organización concreta.

Con el fin de apoyar a las administraciones públicas para que lleven a cabo sus propias evaluaciones de riesgos, se ha incluido una lista de amenazas en el Anexo IV.

El análisis no tiene en cuenta ningún requisito específico y está concebido como una primera evaluación general de los diferentes posibles candidatos como modelos de implementación en la nube. Al leer este capítulo, el lector debe tener la información necesaria para identificar el modelo de nube más adecuado a sus circunstancias. Entonces, se puede realizar una evaluación más detallada del modelo adoptado.

En el capítulo 4, donde se tienen en cuenta los requisitos específicos de cuatro ejemplos de servicios (servicios sanitarios electrónicos, procedimientos administrativos electrónicos, correo electrónico y aplicaciones de recursos humanos), se ha proporcionado un asesoramiento más concreto.

4.1 Nube pública

Puntos fuertes

El modelo de nube pública parece ser el mejor posicionado para ofrecer una gran resistencia, en particular con respecto a las cifras de rendimiento y fiabilidad. De forma más detallada, podemos decir lo siguiente:

- Disponibilidad y fiabilidad: la mayor agrupación de recursos simplifica el manejo y el enmascaramiento de fallos en recursos de hardware y ofrece unas cifras más altas de fiabilidad del servicio implementado.

- Tolerancia y elasticidad: la mayor agrupación de recursos simplifica el manejo de la pérdida de rendimiento debida a los picos en la demanda, puesto que el servicio de interés puede explotar recursos disponibles para evitar una caída en el rendimiento para los usuarios finales. Sin embargo, esto requiere el diseño y la implementación adecuados de la aplicación y el control correcto de la aplicación para detectar pérdidas en el rendimiento de la aplicación del usuario. El seguimiento es fundamental para la explotación de los recursos de la nube y la consecución del cumplimiento de objetivos.

- Administración de parches: SaaS puede garantizar el mejor rendimiento en el tiempo medio entre parches. En SaaS, los usuarios tienen menos responsabilidad, pero deben introducirse los controles adecuados para garantizar que los parches se aplican realmente. En Iaas y PaaS, los usuarios tienen un mayor grado de responsabilidad[17].

- Tiempo de respuesta: los rendimientos en términos de fiabilidad y elasticidad que se pueden lograr mediante la correcta reconfiguración de una aplicación hacen que sea posible explotar mejor los recursos disponibles de modo que el tiempo de respuesta para el usuario final pueda siempre mantenerse dentro de un intervalo predefinido.

- Continuidad del negocio: los recursos de una nube pública implementada por un gran proveedor pueden ser distribuidos geográficamente. Esto simplifica la definición de continuidad del negocio y las estrategias de recuperación ante desastres.

- Seguridad física: se puede lograr un grado muy elevado de seguridad en cada sitio del proveedor gracias a que nadie está autorizado a realizar una auditoría en el sitio y porque se puede implementar un fuerte control sobre el acceso físico.

- Prevención y detección de intrusiones: dada la gran cantidad de recursos en la nube, algunos de estos pueden dedicarse a la vigilancia de la integridad y a la detección de intrusiones para descubrir los ataques maliciosos sin que por ello disminuya el rendimiento final al usuario.

[17] *La atribución de responsabilidad fue analizado en las páginas 64-65 del informe de ENISA del año 2009.*

- Las fuertes medidas de seguridad física pueden permitir al proveedor retrasar posibles órdenes judiciales de comparecencia y procesos de obtención de datos (*e-discovery*) por parte de las autoridades policiales de otros países.

La mayor parte de los beneficios se deben al gran tamaño de la agrupación de recursos disponibles y a su distribución geográfica (como ya se mencionó en el informe sobre los beneficios y los riesgos de seguridad publicado por ENISA en 2009). La homogeneidad de los recursos utilizados para construir la nube puede fortalecer y simplificar el diseño y la gestión de todo el sistema. Esto implica que los puntos fuertes son directamente proporcionales a la escala del proveedor de la nube. No es realista imaginar que, en un futuro próximo, los proveedores de nube pública ofrezcan servicios de nube privada más específicos para las administraciones públicas que los que están ofreciendo ahora.

Puntos débiles

Los principales puntos débiles de una solución en la nube pública para las organizaciones gubernamentales están relacionados con la falta de gobernabilidad, el gran número de abonados (usuarios) en la nube y el fuerte poder de negociación del proveedor de la nube en la definición del contrato. Más detalladamente, algunos de los principales puntos débiles del modelo de nube pública desde la perspectiva de un organismo público son los siguientes:

- La falta de cumplimiento legal y reglamentario (retención de datos, informática forense, presentación de informes): estas amenazas se agravan en los modelos SaaS y PaaS, donde el usuario tiene menor control, gobernabilidad y visibilidad sobre la infraestructura.

- Falta de control sobre la cadena de suministro: cabe señalar que, en el caso de IaaS, el control sobre la cadena de suministro para la provisión del servicio es mayor que en PaaS y SaaS, pero este beneficio potencial siempre debe ser comparado con los costes adicionales generados por la plataforma y la gestión de la seguridad del software y la resistencia.

- Capacidades de registro: los proveedores de la nube pública normalmente no ofrecen una capacidad de registro suficientemente detallada sobre las operaciones y la administración de la nube y, quizás lo más importante, hay una falta de información sobre respuesta ante incidentes e informática forense.

- Dificultades para acceder a datos de informática forense para determinar la *linkability* y la rendición de cuentas (*accountability*) en los casos en que se llevan a cabo actividades ilegales.

  Falta de la capacidad de negociación necesaria por parte de determinados organismos públicos en la negociación de los términos y las condiciones y en la solicitud de un nivel suficiente de transparencia por parte del proveedor o proveedores.

- Requisitos legales y reglamentarios específicos que, en algunos países, obligan a las organizaciones públicas a mantener los datos dentro del territorio nacional y a reducir el grado de continuidad del negocio que se puede alcanzar.

- El deterioro del rendimiento (IaaS, PaaS y SaaS) debido a la mala calidad en la estructuración de una aplicación y su capacidad para explotar de forma dinámica los recursos disponibles con el fin de manejar los fallos y/o los picos de demanda.

- El deterioro del rendimiento (IaaS, PaaS y SaaS) debido a la mala calidad de la conectividad (p. ej., zonas rurales, especialmente en los países del sur y el este de la UE). Esto solo se aplica en los casos en los que el cliente está situado en áreas específicas. Para los clientes más distribuidos esto no es un problema.

- Distribución local limitada de los centros de datos en el territorio de la UE, que puede influir en el rendimiento del servicio. Estas consideraciones pueden ser especialmente ciertas en una situación en la que una autoridad pública esté ubicada en un lugar remoto (p. ej., ENISA en Creta) que puede sufrir con mayor probabilidad un deterioro del rendimiento debido a la mala calidad de la conectividad.

- Dificultades para transferir datos de vuelta al usuario o al proveedor alternativo elegido de servicios en la nube. Estas dificultades pueden ser un problema grave, especialmente para los servicios de sanidad, en los que un fallo o un retraso en la transferencia de información relacionada con la salud puede representar una seria amenaza para la autoridad sanitaria, así como para los pacientes.

Oportunidades

En comparación con las soluciones internas, las nubes públicas podrían ofrecer oportunidades para mejorar las prácticas actuales de los potenciales usuarios gubernamentales, en las áreas de preparación y cumplimiento legal y, más aún, en particular en:

- Análisis y evaluación de riesgos
- Pruebas de seguridad
- Supervisión de la seguridad en tiempo real
- Informática forense (por favor, téngase en cuenta que la aparente contradicción de incluir 'informática forense' tanto en los puntos débiles como en las oportunidades se debe al hecho de que en la actualidad estos servicios no son ofrecidos por los proveedores de nubes, pero se podrían convertir en un factor en la diferenciación de las ofertas en un futuro próximo, por lo que lo vemos como una oportunidad) (15).

Esto se debe a las siguientes razones:

- Es difícil contar con personal interno especializado para llevar a cabo, de forma periódica, los análisis y las evaluaciones de riesgo, así como las pruebas de seguridad.
- Contar con los recursos necesarios para construir un centro de operaciones de seguridad interno para supervisar la seguridad en tiempo real o bien adquirir estos servicios en el mercado, es costoso.

- Las presiones del mercado o de los competidores que obliguen a los proveedores de nube pública a ofrecer funciones de seguridad representará un valor añadido para los clientes.
- Presión ante el cumplimiento.

Para que una nube pública pueda aprovechar estas oportunidades, se deben tomar las siguientes medidas:

- Control total sobre los inventarios de bienes.
- Clasificación detallada de los activos físicos, información y servicios.
- Integración entre el análisis/evaluación de riesgos y los procesos de supervisión de la seguridad en tiempo real.
- Inspección eficaz de los empleados del proveedor.

Amenazas

Diversas amenazas se ciernen sobre el modelo de nube pública, y la mayoría de ellas ya han sido identificadas por ENISA, así como por otras organizaciones (p. ej., la Cloud Security Alliance, y el grupo de interés LinkedIn).
Las mayores amenazas a las que se enfrentan las autoridades públicas al seleccionar una solución de nube pública son:

- Una gran nube pública es un objetivo atractivo para los ataques, debido a la ingente cantidad de información a la que los atacantes pueden acceder tras el éxito de sus ataques. El tamaño de esta información justifica una inversión incluso mayor en tiempo y en recursos para poner en práctica el ataque.

- El impacto de los ataques por amenazas de seguridad internas puede ser bastante elevado debido a la cantidad de información almacenada en la nube. Se deben conservar los registros detallados de las actividades internas, el proveedor debe adoptar políticas de rotación en el empleo y también se deben adoptar políticas de necesidad de saber.

- Un fallo de aislamiento (15) puede provocar una salida de información (seguimiento ilegal) así como problemas de funcionamiento debidos a la falta de aislamiento de los recursos de otros abonados. En este caso, puede producirse una pérdida de información como resultado de un ataque contra otro usuario de la nube pública.

- La inadecuada definición de los requisitos y de la clasificación de los activos puede provocar la exposición de los activos a otros usuarios de la nube.

- Se pueden aplicar múltiples jurisdicciones cuando los sitios del proveedor estén distribuidos entre varios países.

- Un cambio en el control del proveedor puede dar lugar a la adopción de distintas estrategias de seguridad así como a estrategias de comercialización diferentes que se traduzcan en una menor calidad del servicio.

- En las soluciones SaaS o PaaS se puede adoptar un formato propietario para almacenar datos en la nube. El traslado a otro proveedor puede ser casi imposible si no existe una herramienta que traduzca automáticamente los datos al nuevo formato.

En el ANEXO IV se puede encontrar una lista detallada de las amenazas aplicables a todos los modelos de nube.

3.5. Nube privada

Puntos fuertes

En una nube privada, el usuario-propietario tiene, en principio, el control absoluto (sujeto a las limitaciones económicas) sobre el conjunto de características de la implementación de la nube; sin embargo, existen costes (que no pueden ser compartidos con otros clientes) asociados a este aumento en el control.

La siguiente lista contiene las características más importantes (sobre seguridad y resistencia) que se pueden definir en una nube privada:

- Prácticas de evaluación de riesgos: es posible seleccionar las metodologías, escalas, criterios de medición, etc.

- Parches: es posible programar parches cuando sea necesario, y también modificar el régimen.

- Control de acceso: Granularidad más fina de la gestión y las políticas de acceso para evitar fugas de datos.

- Registro: es posible controlar lo que se registra, dónde se almacena, cómo se protege el almacenamiento y durante cuánto tiempo se guardará.

- Auditoría: es posible establecer y regular el derecho a auditar.

- Control sobre la disponibilidad, fiabilidad, escalabilidad y elasticidad: el cliente puede especificar el sistema y definir los acuerdos de nivel de servicio para que la nube privada se ajuste, dentro de las limitaciones técnicas, al rendimiento de servicio requerido.

- Disponibilidad de la interfaz de gestión: se puede negociar más fácilmente con los proveedores de servicios de Internet los servicios de primera calidad para obtener una red y una conexión mejores (p. ej., prioridad en la reanudación del servicio).

- Plan de continuidad de negocio: se puede definir el plan y comprobar todos sus componentes.

- Respeto de la legislación: una total transparencia y control sobre los requisitos legales, como la ubicación de datos.

Puntos débiles

- El efecto beneficioso de las economías de escala en las nubes privadas es probable que sea mucho menor en comparación con las nubes públicas (por lo menos las de gran escala, presentes actualmente en el mercado) o incluso con las comunitarias.

- La posible falta de una escala adecuada también representa un punto débil en la adquisición y la puesta en marcha de mecanismos de seguridad.

- Existe, en potencia, una menor tolerancia a los ataques maliciosos que en una nube pública, partiendo del supuesto de que los recursos disponibles (especialmente en términos de capacidad de computación) pueden ser menos adecuados que los de una nube pública. En algunos casos, también es posible que la experiencia interna del proveedor no sea suficiente.

- Hay menos resistencia para satisfacer los picos de demanda inesperados, debido a la escasez de recursos. Esto requiere planificar la capacidad y una evaluación comparativa antes de trasladarse a la nube.

- Siendo realistas, es posible que una nube privada pueda definir un régimen de redundancia completo; sin embargo, es muy poco probable que esto sea igual o mejor que el régimen de redundancia ofrecido por la nube pública de un importante proveedor de nube.

- La falta de geo-redundancia es un problema en cuanto a la continuidad del negocio. En general, el tiempo que tarda en recuperarse de un fallo una nube privada puede ser bastante superior al de una nube pública, a menos que el proveedor implemente mecanismos y políticas específicos. En este sentido, debe definirse un acuerdo de nivel de servicio adecuado con el proveedor.

- Sensibilidad de la reputación: la reputación de los gobiernos y los organismos públicos puede ser extremadamente sensible a la fuga de información y a cualquier incidente de seguridad, incluido el uso de una infraestructura propiedad de las administraciones públicas para lanzar ataques maliciosos.

Oportunidades

- Seguimiento: en una nube privada, los mecanismos de seguimiento orientados al usuario y las aplicaciones se pueden implementar realizando un ajuste rápido de los recursos para cubrir los posibles picos de demanda. Además, se pueden controlar por completo los eventos de

seguridad de interés. Como contrapartida, si la escala de la nube privada no es la apropiada, el manejo de los picos de demanda de recursos puede ser bastante complejo y no existe una solución eficaz para los picos imprevistos. No obstante, los recursos de la nube deben ser explotados para mejorar el rendimiento de las aplicaciones que se trasladen a la nube.

- Control de acceso: si es necesario, se pueden adoptar más fácilmente políticas de acceso basadas en sistemas de control de acceso no discrecional (p. ej., MAC (control de acceso obligatorio) o RBAC (control de acceso basado en roles)) para limitar aún más a cada usuario y minimizar los flujos ilegítimos entre usuarios.

Amenazas

Un gobierno o un organismo público dispuesto a crear y utilizar una nube privada debe estar preparado para enfrentarse a las siguientes amenazas:

- Ataques con motivos políticos: mientras que la cantidad de información gestionada por la nube puede no resultar atractiva por sí misma, el deterioro de un sitio del gobierno puede ser atractivo por motivos políticos. (Obviamente, esta amenaza no se limita a las nubes privadas, pero una nube gubernamental privada podría presentar una concentración muy elevada de recursos y, por lo tanto, el incentivo para un atacante motivado sería aún mayor).

- Efecto gran hermano: el hecho de que las administraciones públicas recopilen y gestionen información acerca de los ciudadanos y, a la larga, de las empresas (en caso de que la nube se utilice como un vivero de empresas para las pymes) puede ser percibido, desde la perspectiva del usuario final, como un modo posible de establecer un sistema de vigilancia y de creación de perfiles.

- La alta volatilidad en la utilización de recursos y los picos inesperados en las solicitudes podría obligar a una nube privada a escalar horizontalmente a una nube pública (nube híbrida), fuera del alcance de la política de seguridad definida. En tal caso, el control sobre la información en la nube se pierde parcialmente siempre que no se defina la política de seguridad, que marca las normas sobre la información que se puede exportar.

- Mala planificación: por ejemplo, la definición de los requisitos y la clasificación de los activos puede originar una pérdida de seguridad e integridad cuando se pasa de una nube privada a una nube híbrida.

- La definición inadecuada de los contratos con los socios comerciales (operador de nube, socios tecnológicos, proveedores de hardware y software, etc.) y la falta de seguimiento de la ejecución de los contratos puede ser crítica en relación con el tamaño del proveedor.

3.6. Nube comunitaria

Al analizar una nube comunitaria, se debe considerar que, en principio, sus puntos fuertes y débiles se encuentran entre los de una nube privada y los de una pública. En general, el conjunto de recursos disponibles es mayor que en una nube privada, con ventajas evidentes en términos de elasticidad. Sin embargo, el conjunto no es tan grande como el de una nube pública, y esto limita la elasticidad que ofrece una nube comunitaria. Por otro lado, el número de usuarios en una nube comunitaria es mucho menor que en una nube pública, lo que tiene ventajas obvias en términos de seguridad.

Puntos fuertes

- Requisitos y limitaciones comunes y perfil de riesgo: los usuarios de una nube comunitaria tienen requisitos similares desde una perspectiva de seguridad y rendimiento. Esto hace que la implementación de las políticas para satisfacer dichos requisitos sean más eficientes y rentables, incluso para el proveedor, lo que se traduce en un menor coste global.

- Los requisitos y los perfiles de riesgo comunes simplifican la configuración de mecanismos y herramientas para proteger las aplicaciones que se ejecutan en la nube de ataques internos y externos.

- Los usuarios tienen más poder de negociación como grupo (en relación con el proveedor de nube) debido al mayor número de usuarios con necesidades similares.

- Capacidad para establecer los criterios de inclusión: la membresía se otorga de acuerdo con la resistencia de los miembros potenciales. Esto reduce mucho los riesgos debidos a ataques de otros usuarios de la nube.

- Una mayor escala y una mejor respuesta a los picos elevados de demanda de recursos (en comparación con una nube privada): el tamaño de las agrupaciones de recursos puede ser notablemente mayor que el de una nube privada y esto simplifica la gestión de los picos de demanda de recursos.

Puntos débiles

- Existe más competencia por los recursos entre los socios, ya que tienen objetivos comunes. Algunos de los beneficios derivados del hecho de disponer de un mayor número de recursos se pierden porque los usuarios de la misma comunidad pueden presentar patrones similares a la hora de acceder a los recursos, por lo que se pueden producir en un mismo espacio de tiempo picos de solicitudes de recursos por parte de varios usuarios.

- En comparación con una nube privada, una comunidad es un objetivo más atractivo para los atacantes motivados debido a la mayor visibilidad alcanzada por los ataques con éxito. Además, las aplicaciones de otros usuarios pueden proporcionar una vía para los ataques.
- El control de acceso y la autenticación están debilitados en comparación con una nube privada debido al mayor número de usuarios.

- El deterioro del rendimiento (IaaS, PaaS y SaaS) debido a la mala calidad de la conectividad (p. ej., zonas rurales, especialmente en los países del sur y el este de la UE) puede reducir la calidad del servicio para algunos usuarios de la comunidad (que no estén ubicados cerca de los puntos de suministro), en comparación con una nube privada.

Oportunidades

- Los requisitos similares que se registran en la comunidad (véanse los puntos fuertes) podrían permitir la mejora de las políticas, los parámetros de referencia y las normas de seguridad, así como prácticas comunes para el análisis y la evaluación de riesgos, el registro y el seguimiento. Esto puede dar lugar a implementaciones altamente eficientes que reducen el coste de adopción para cada usuario y propician una arquitectura más fiable.

- Los sistemas de gestión de incidentes comunes y compartidos pueden simplificar la adopción de mecanismos para almacenar y administrar las pruebas informático-forenses.

- El intercambio de información entre otros miembros de la comunidad (las mejores prácticas de uso, la experiencia de incidentes anteriores, etc.) puede propiciar una mayor difusión de las mejores prácticas, ajustada por los miembros más expertos de la comunidad.

- Se puede obtener una seguridad más estricta porque la información sobre las políticas de seguridad y el diseño y la implementación de la nube solo se comparte dentro de la comunidad. En comparación con una nube pública, esto incrementa la dificultad, para un atacante, de adquirir información para poner en práctica sus ataques.

Amenazas

- Falta de acuerdo sobre las líneas básicas de la seguridad y los mecanismos de seguridad: para aprovechar la oportunidad de compartir mecanismos para proteger y defender la información, se debe negociar un acuerdo entre todos los miembros de la comunidad. La mayoría de las veces, una renegociación, incluso aunque abarque a un número reducido de usuarios, puede ser bastante compleja y no tener éxito.

- Las comunidades pueden crecer demasiado deprisa, lo que a la larga reduce las ventajas de la nube comunitaria en términos de resistencia, en comparación con una nube privada, o pueden crecer muy lentamente, lo que eventualmente afectará a la escalabilidad dinámica.

- Más difícil predicción del uso de recursos (que en una nube privada): el mayor número de usuarios incrementa la complejidad de anticiparse a las solicitudes de recursos de cada usuario. En una nube comunitaria, es más probable que se produzcan errores en la planificación de la capacidad de la nube.
- Un fallo en los mecanismos de aislamiento puede causar la filtración de información, que es más difícil de controlar debido al mayor número de usuarios.

- Es difícil identificar a la entidad jurídica que es responsable de actuar contra un miembro de la comunidad o el proveedor cuando están implicados asuntos supranacionales.

Situaciones hipotéticas que sirven como ejemplo

En este capítulo se expone la esencia del modelo sencillo de toma de decisiones con tres situaciones hipotéticas. Estas situaciones ficticias se basan en parte en experiencias concretas de la vida real.

Las situaciones se basan en los siguientes casos prácticos de uso:

- Nube sanitaria: el uso de la computación en la nube para implantar un servicio de historias clínicas electrónicas para autoridades sanitarias nacionales, regionales y locales;
- Autoridades locales y regionales.
- Nube gubernamental como un vivero de empresas.

En aras de la brevedad, solamente se ha incluido en este capítulo una descripción y análisis de cuatro ejemplos de servicio que son representativos de estas situaciones hipotéticas: 1) Historia clínica electrónica (HCE), 2) Procedimiento administrativo electrónico (PAE), 3) correo electrónico y 4) aplicaciones de recursos humanos

Para más detalles sobre las situaciones hipotéticas, se puede consultar el Anexo II.

5.1 Descripción del servicio

Historia clínica electrónica (HCE)

La Historia Clínica Electrónica (HCE) es un almacén de información sobre el estado de salud de un paciente en un formato procesable por el ordenador, guardado y transmitido de forma segura y accesible por múltiples usuarios autorizados. Posee un modelo lógico de información normalizado o decidido de común acuerdo que es independiente de los sistemas de HCE. Su objetivo principal es el apoyo a la atención sanitaria integrada continua, eficiente y de calidad y contiene información que es retrospectiva, concurrente y prospectiva (22).

- La HCE representa para los médicos una fuente de información centralizada en el paciente que es segura, en tiempo real y procede del centro de atención.
- La HCE ayuda a los médicos a tomar decisiones mediante el acceso a la información registrada sobre la salud de los pacientes donde y cuando la necesiten y mediante la incorporación de ayuda para la toma de decisiones basada en la evidencia.

- La HCE automatiza y racionaliza el flujo de trabajo clínico, cerrando bucles en la comunicación y la respuesta que puede dar lugar a retrasos o deficiencias en la atención.

La HCE también puede simplificar la recopilación de datos para usos distintos a la atención clínica directa, tales como facturación, gestión de la calidad, informes de resultados, planificación de recursos y vigilancia de enfermedades que afecten a la salud pública y sus correspondientes informes.

Los requisitos esenciales de la HCE (23) son los siguientes:

- Proporcionar un acceso seguro, fiable y en tiempo real a la información de la historia clínica del paciente donde y cuando se necesite para ayudar en la atención a dicho paciente.
- Garantizar la confidencialidad y seguridad de la información sanitaria del paciente.
- Ser accesible y fiable en todo momento.
- Ser lo suficientemente adaptativa para integrarse con el flujo de trabajo clínico.
- Ser accesible cuando se necesite, en hospitales y ambulatorios, con acceso remoto.

Procedimiento administrativo electrónico (PAE)

El procedimiento administrativo electrónico (PAE) se refiere en esencia a las tareas de envío electrónico, y a servicios de documentación sobre la interacción de las administraciones públicas con los ciudadanos, las empresas y otras áreas de las administraciones públicas. Técnicamente, describe la gestión electrónica de los procedimientos administrativos relativos a archivos y registros.

Como tal, el PAE comprende, por ejemplo, solicitudes en línea en materia de subvenciones, ayudas, licencias, certificados o formularios y, para apoyar estas solicitudes, puede permitir:

- La presentación de las solicitudes.
- La recuperación y el acceso a la información del estado de las órdenes o los procesos.
- El acceso interactivo a las solicitudes o procesos pendientes-
- La información sobre las interacciones o los documentos necesarios.
- Facilidades para proporcionar información o suministrar documentos directamente.
- Notificaciones.
- Recuperación de documentos y formularios.
- Pagos electrónicos.

Una descripción detallada de estos servicios, así como otros servicios ofrecidos por organizaciones públicas que se tienen en cuenta en este informe, está publicada en el Anexo II, junto con las situaciones de los casos prácticos.

Correo electrónico

El correo electrónico es el conocido medio de comunicación utilizado para el intercambio de mensajes digitales.

El correo electrónico es considerado en muchas organizaciones como un servicio crítico del negocio y, a menudo, se intercambia información confidencial por correo electrónico.

Aplicaciones de recursos humanos

Las aplicaciones de recursos humanos son aquellos servicios de TI que proporcionan apoyo a la gestión de los recursos humanos. Consisten en el seguimiento de los datos existentes de los trabajadores, lo cual incluye tradicionalmente las historias personales, aptitudes, capacidades, logros y salario. Los sistemas de gestión de recursos humanos abarcan los siguientes elementos:

- Nómina
- Tiempo de trabajo
- Administración de beneficios
- Sistemas de gestión de la información de recursos humanos
- Contratación
- Sistemas de gestión de la formación y de gestión del aprendizaje (SGA)
- Registros de rendimiento

El módulo de nómina automatiza el proceso de pago mediante la recopilación de datos sobre las horas de trabajo y la asistencia al trabajo del empleado, calcula las diversas deducciones e impuestos y genera cheques periódicos de pago e informes fiscales del trabajador. En general, los datos se recopilan a partir de los módulos de recursos humanos y de control de la puntualidad para calcular los depósitos automáticos y las capacidades manuales de emisión de cheques. Este módulo puede abarcar todas las transacciones relacionadas con los empleados, así como la integración con los sistemas de gestión financiera existentes.

El módulo del tiempo de trabajo recopila el tiempo de trabajo estandarizado y los esfuerzos relacionados con el trabajo. Los módulos más avanzados proporcionan una gran resistencia en los métodos de recopilación de datos, capacidades de distribución laboral y características de análisis de datos. Las principales funciones son el análisis de costes y la medición de la eficiencia.

El módulo de administración de prestaciones proporciona un sistema para que las organizaciones administren y controlen la participación de los empleados en los programas de prestaciones. Algunas de ellas suelen ser seguros, indemnizaciones, reparto de beneficios y jubilación.

El módulo de gestión de recursos humanos es un componente que abarca muchas otras funciones de recursos humanos, desde solicitudes de empleo hasta jubilación. El sistema registra datos básicos sobre demografía y domicilio, selección, formación y desarrollo, gestión de capacidades y conocimientos, registros de planificación de compensaciones y otras actividades relacionadas. Los

sistemas más avanzados tienen la capacidad de 'leer' las solicitudes de empleo e introducir los datos pertinentes en los campos de una base de datos, notificar a los empleadores y facilitar la gestión y el control del puesto. La función de gestión de recursos humanos consiste en la contratación, colocación, evaluación, compensación y desarrollo de los empleados de una organización.

La contratación en línea se ha convertido en uno de los primeros métodos empleados por los departamentos de recursos humanos para reunir a candidatos potenciales para los puestos disponibles dentro de una organización.

El módulo de formación proporciona un sistema para que las organizaciones administren y controlen los esfuerzos en formación y desarrollo realizados por sus empleados. Sofisticados sistemas de gestión del aprendizaje (SGA) permiten a los administradores aprobar la formación, presupuestos y calendarios junto con la gestión y evaluación del rendimiento (24).

3.7. Parámetros y requisitos

Las organizaciones gubernamentales y las autoridades locales ficticias consideradas en este informe deberían tener en cuenta algunos parámetros clave a la hora de evaluar el impacto en el coste/beneficio de una estrategia de nube en los servicios de seguridad y recuperación.

En la tabla "Atributos del servicio" incluida en el Anexo III, se sugieren una serie de parámetros de carácter general y se indican los requisitos asociados para el tipo de servicio considerado. Cabe señalar que:

- Una vez más, los parámetros deben entenderse solo como ejemplos de posibles combinaciones de las variables mencionadas en el capítulo 3 (Modelo para la toma de decisiones). Esto tiene como objetivo ser instructivo para el lector y mostrarle cómo interpretar las variables anteriores.
- Los requisitos se derivan de las respuestas directas a cuestionarios respondidos por autoridades locales y regionales y autoridades sanitarias o están basados en la experiencia de los miembros del grupo de expertos.

Ejemplo de servicio

	HCE	PAE Procedimientos administrativos electrónicos	Correo electrónico	Aplic. recursos humanos
Parámetros	**Requisitos**			
Sensibilidad de los datos				
Tipo de datos	Datos Personales Datos sensibles	Datos Personales Datos sensibles	Datos Personales Datos empresariales	Datos Personales Datos sensibles
Requisitos de seguridad y resistencia de la información	Integridad Alta Confidencialidad Alta Disponibilidad Alta	Integridad Alta Confidencialidad Alta Disponibilidad Media	Integridad Media Confidencialidad (específica de contenido) Disponibilidad Media	Integridad Alta Confidencialidad Alta Disponibilidad Media
Escalabilidad – Gestión de la demanda				
Volatilidad de la demanda	Alta (para almacén accesible por pacientes e investigadores) Baja (para HCE)	Alta	Media	Media
Nuevos servicios requeridos	Sí	Sí	No	No
Prevención de las necesidades de almacenamiento para los próximos cinco años	Predecible	Predecible	Predecible	Predecible
Pico de usuarios concurrentes	Alto	Alto	Alto	Medio
Proporción de los datos en uso activo	Bajo	Medio	Bajo	Medio
Nivel de acceso administrativo (usuario privilegiado – dpto. de TI) requerido	Bajo	Bajo	Bajo	Bajo [18]
Fiabilidad del servicio – Disponibilidad y rendimiento en caso de dificultades (*performability*)				
Disponibilidad requerida	99,9% (Alta)	98% (Media)	97% (Media)	98% (Media)
Requisitos de	Muy breve –	Menos de	Menos de	Menos de

[18] *Partiendo de la base de que para el sistema se ha diseñado una arquitectura adecuada*

tiempo de inactividad no planificado	menos de una hora	4 horas	2 horas	4 horas
Respuesta en tiempo real	Baja	Media	Media	Media
Colaboración e interoperabilidad				
Otras autoridades sanitarias y administraciones públicas necesitan acceder al servicio	Sí	Sí	No	Sí
Gestión de identidades, autenticación y acceso				
Gestión de identidades	Las identidades de los pacientes deben gestionarse internamente	Las identidades de los ciudadanos se pueden gestionar internamente o mediante un proveedor externo (p. ej., proveedor de la nube)	Las identidades del usuario se pueden gestionar internamente o mediante un proveedor externo (p. ej., proveedor de la nube)	Las identidades del usuario se pueden gestionar internamente o mediante un proveedor externo (p. ej., proveedor de la nube)
Provisión de credenciales y permisos para los usuarios	El proceso de provisión de credenciales y permisos para los usuarios (pacientes, médicos, personal de administración, etc.) debe ser gestionado internamente	El proceso de provisión de credenciales a los usuarios (ciudadanos, personal administrativo, etc.) puede ser gestionado internamente o mediante un proveedor externo (p. ej., proveedor de la nube)	El proceso de provisión de credenciales a los usuarios puede ser gestionado internamente o mediante un proveedor externo (p. ej., proveedor de la nube)	El proceso de provisión de credenciales a los usuarios puede ser gestionado internamente o mediante un proveedor externo (p. ej., proveedor de la nube)
RBAC	SÍ	SÍ	NO	SÍ
Solidez de la autenticación	Alta Requisito legal	2 factores de autenticación (opcionalmente)	Media	Contraseña (opcional)
Se requiere federación	Sí	Sí	No	No
Cifrado				
Cifrado	SÍ en el tránsito – se recomienda cifrar el	Opcional	Opcional	Recomendado en el tránsito (según

	resto según los requisitos legales			normativa)
Acceso a las claves				
Provisión de credenciales y permisos para acceder a la administración	Proveedor para proporcionar credenciales de autenticación para el acceso a la administración	Proveedor para proporcionar credenciales de autenticación para el acceso a la administración	Proveedor para proporcionar credenciales de autenticación para el acceso a la administración	Proveedor para proporcionar credenciales de autenticación para el acceso a la administración
Legalidad y cumplimiento				
Protección de datos	Aplicable	Aplicable	Aplicable	Aplicable
Localización de datos y jurisdicción legal	Ambos deben ser especificados (la ley en algunos países impone el requisito de que los datos no pueden salir del territorio nacional)	Ambos deben ser especificados (la ley en algunos países impone el requisito de que los datos no pueden salir del territorio nacional)	Ambos deben ser especificados (la ley en algunos países impone el requisito de que los datos no pueden salir del territorio nacional)	Ambos deben ser especificados (la ley en algunos países impone el requisito de que los datos no pueden salir del territorio nacional)
Control de acceso	Se debe establecer una combinación de sistemas de control de acceso obligatorio (MAC) [19] y de control de acceso basado en roles (RBAC).	Se debe establecer un sistema de control de acceso obligatorio (MAC) o un RBAC.	Se debe establecer un sistema de control de acceso obligatorio (MAC) o un RBAC.	Se debe establecer un sistema de control de acceso obligatorio (MAC) o un RBAC.
Rendición de cuentas (*accountability*) (registros admisibles en un tribunal)	SÍ	SÍ	SÍ	SÍ
Acceso mediante ID digital (carnet de	SÍ	SÍ	NO	NO

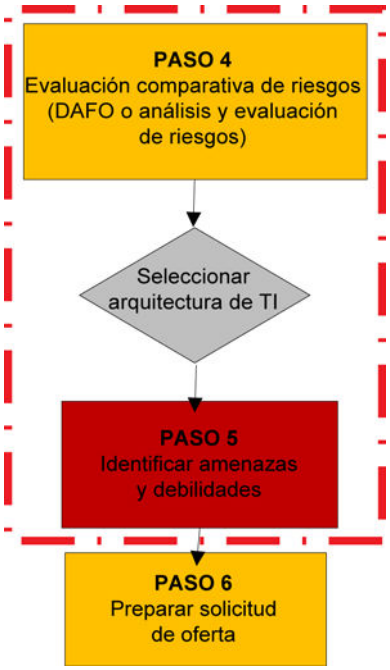
[19] Se ha sugerido el sistema MAC como requisito para la HCE por las razones siguientes: 1) El paciente es el propietario de su HCE y debe ser capaz de decidir: a) quién puede acceder a qué tipo de datos y b) a quién delega esta decisión. 2) La confidencialidad y la integridad tiene una importancia fundamental en la HCE, y el paciente debe ser capaz de hacer cumplir las reglas acerca de cualquier posible acceso a niveles superiores o más allá del modelo de propiedad (p. ej., superusuario o *root* en un sistema UNIX). Basándose en estos supuestos, el sistema MAC parece ser más apropiado que, por ejemplo, un control de acceso discrecional, dada la posibilidad que ofrece MAC de establecer las normas definitivas de acceso. Para más información, véase: (http://en.wikipedia.org/wiki/Discretionary_Access_Control), (http://en.wikipedia.org/wiki/Mandatory_Access_Control) y (http://en.wikipedia.org/wiki/Role-Based_Access_Control).

identidad de ciudadano)				
Firma digital	SÍ	Los procesos y documentos deben ser validados con una firma digital (internamente o por los ciudadanos). Los proveedores sanitarios están firmando los datos.	Los correos electrónicos oficiales se pueden firmar digitalmente.	NO
SSO – *single sign-on*	Opcional	Opcional	Opcional	Opcional
No repudio	SÍ	SÍ	SÍ	SÍ
Consignación de fecha y hora electrónica	Sí – necesaria para registros de auditoría, etc., para investigaciones médicas	Algunos documentos (p. ej., permisos, licencias, pagos, etc.) presentados o emitidos, deben tener un sello de fecha y hora concedido por una autoridad certificada.	NO	NO
Contraseñas únicas o nombres de usuario únicos	SÍ	SÍ	SÍ	SÍ
Aplicación del principio de la necesidad de saber (aplicación)	SÍ	SÍ	SÍ	SÍ
Transparencia de la cadena de suministro	Se requiere total transparencia frente a terceros proveedores.	Se requiere total transparencia frente a terceros proveedores.	Se requiere total transparencia frente a terceros proveedores.	Se requiere total transparencia frente a terceros proveedores.
Diligencia debida de la cadena de suministro	SÍ	SÍ	SÍ	SÍ

TABLA 1: ATRIBUTOS DEL SERVICIO

5.3. Evaluación comparativa de riesgos

En este apartado, realizamos un análisis comparativo de las nubes públicas, privadas y comunitarias para averiguar qué tipo de nube, en el contexto de las situaciones hipotéticas propuestas, podría ser la solución más adecuada para satisfacer las necesidades de servicio descritas en el apartado 5.2.
Como ya se explicó al principio de este capítulo, las necesidades de servicio en las que se basa la evaluación representan solo posibles configuraciones de situaciones de la vida real y no deben considerarse análisis concretos tal cual. Demuestran cómo puede utilizarse la metodología de este documento para tomar una decisión.



Como los cuatro servicios presentan requisitos similares, hemos reflejado en la tabla siguiente solo una evaluación comparativa del servicio HCE. Sin embargo, también hemos incluido una referencia a los otros servicios, mencionando sus características específicas.

Historia clínica electrónica (HCE)
Parámetro: Importancia y sensibilidad de los datos
Requisito
HCE: al facilitar historias clínicas electrónicas, una autoridad sanitaria gestiona datos personales y sensibles. Los requisitos de resistencia y seguridad de la información para el servicio HCE son alta integridad, alta confidencialidad y alta disponibilidad. Además, el no repudio y los registros de auditoría son requisitos cada vez más importantes en las HCE.

PAE, CORREO ELECTRÓNICO y APLICACIONES DE RECURSOS HUMANOS: Los requisitos de resistencia y seguridad de la información para estos servicios son alta integridad, alta confidencialidad y disponibilidad media.		
Comunitaria	**Privada**	**Pública**
HCE: El modelo de nube comunitaria tiene puntos fuertes similares a una nube privada en cuanto al control sobre los datos, confidencialidad e integridad, pero si hay que compartir entre miembros de la comunidad, entonces el debilitamiento de la política de seguridad de varias islas de nubes privadas (o infraestructuras de TI internas) para poder compartir puede provocar problemas de seguridad y conflictos de políticas que crean un entorno más inseguro que una nube comunitaria, donde los controles y políticas de seguridad se adaptan a la comunidad. También puede ofrecerse un alto nivel de disponibilidad, especialmente si la escala de infraestructuras de la comunidad es adecuada. Una federación de nubes aporta beneficios de resistencia en cuanto a disponibilidad, elasticidad y gestión de incidencias. Hay que señalar que una federación de islas de nubes privadas combinada con cierto tipo de capa de gestión de comunidades virtuales puede ser una mejor opción que una comunidad alojada cuando se requiere un equilibrio entre servicios compartidos y privados separados pero interdependientes. La falta de confianza entre miembros es una seria amenaza al buen funcionamiento de una nube	HCE: Una nube privada parece la mejor solución para garantizar el control total sobre la integridad y confidencialidad de los datos. El propietario de la nube (por ejemplo, una entidad pública nacional, regional o local) es responsable de crear, gestionar, mantener y supervisar los servicios de TI, y de su evolución. Solo se puede conseguir mejor rendimiento en cuanto a disponibilidad de datos que con los servicios de IT internos si: • La escala de la nube es adecuada. • La nube se gestiona, mantiene y supervisa correctamente. PAE, CORREO ELECTRÓNICO y APLICACIONES DE RECURSOS HUMANOS: Una nube privada parece la mejor solución para garantizar el control total sobre la integridad y confidencialidad de los datos. Al mismo tiempo, una nube privada podría ofrecer fácilmente disponibilidad de datos media. En una nube privada resulta más fácil armonizar y velar por el cumplimiento de la política de seguridad, así como aplicar métodos uniformes de evaluación de riesgos. Una nube privada parece ser la solución que ofrece el entorno más	HCE: Las nubes públicas de gran escala parecen ofrecer una alta disponibilidad de datos. La pérdida de control en infraestructuras (IaaS), y posiblemente plataformas (PaaS) y aplicaciones (SaaS), representa una seria amenaza a la confidencialidad e integridad de datos y el cumplimiento legal. PAE, CORREO ELECTRÓNICO y APLICACIONES DE RECURSOS HUMANOS: Para los requisitos de integridad y confidencialidad se aplican las mismas consideraciones que en el análisis de la sanidad electrónica (es decir, la pérdida de control supone una seria amenaza que requiere consideración especial respecto a las dificultades de introducir el derecho a auditar en contratos). La oportunidad de tener alta disponibilidad, garantizada mediante una nube pública de gran escala, no se

comunitaria. Con la transparencia como principio rector de la comunidad, pueden establecerse y reforzarse relaciones de confianza entre los miembros. PAE, CORREO ELECTRÓNICO y APLICACIONES DE RECURSOS HUMANOS: Ver análisis de HCE. Es discutible si las autoridades locales tendrían poder suficiente para negociar un contrato con proveedores de nubes grandes, aunque aúnen sus necesidades (especialmente de seguridad). Una nube comunitaria tendría menos conocimientos especializados sobre seguridad y mantenimiento que una nube privada pero más nivel de conocimientos respecto a las aplicaciones reales. En concreto, para el servicio de CORREO ELECTRÓNICO: Algunos proveedores de nube pública proporcionan funciones de seguridad como filtrado de contenido, antiphishing, antispam o dejan que los usuarios apliquen sus propias soluciones de seguridad.	estable, una comunidad de interesados, propiedad (el propietario será una organización pública), etc. La oportunidad de tener alta disponibilidad, garantizada mediante una nube pública de gran escala, no se explota completamente al ofrecer un servicio de correo electrónico, ya que requiere un nivel medio de disponibilidad.	explota completamente al ofrecer PAE, ya que requieren un nivel medio de disponibilidad. En concreto, para el servicio de CORREO ELECTRÓNICO: Algunos proveedores proporcionan de nube pública ofrecen funciones de seguridad como filtrado de contenido, antiphishing, antispam o dejan que los usuarios apliquen sus propias soluciones de seguridad.

Parámetro: Escalabilidad y gestión de la demanda		
Requisito		
La infraestructura de TI debe diseñarse para gestionar con rentabilidad: 1) Cargas de trabajo escasas y muy escasas. 2) Picos estacionales (ej., gripe, nóminas, etc.). 3) Picos repentinos e inesperados debidos a cambios en procedimientos administrativos o la aplicación de nuevas leyes y normativas. 4) Implementación de nuevos servicios. 5) Cambios demográficos. 6) Ciberataques e incidentes de TIC.		
Comunitaria	**Privada**	**Pública**
Una nube comunitaria puede ofrecer capacidades de gestión de demanda y	Una nube privada, en función de su escala, es la	Las nubes públicas garantizan un alto nivel

escalabilidad que están a caballo entre las soluciones privadas y públicas. Puede escalar mejor que una nube privada (para satisfacer la demanda) ya que, en principio, existe una infraestructura mayor; sin embargo, no puede explotar completamente economías de escala. PAE: Los requisitos de escalabilidad son iguales que para la HCE. Se aplican las mismas consideraciones.	opción menos adecuada para gestionar eventos inesperados, ciberataques (ej., DDoS) e incidencias de TIC. PAE: Los requisitos de escalabilidad son iguales que para la HCE. Se aplican las mismas consideraciones.	de resistencia y una gestión eficaz de la demanda. PAE: Los requisitos de escalabilidad son iguales que para la HCE. Se aplican las mismas consideraciones.
CORREO ELECTRÓNICO y APLICACIONES DE RECURSOS HUMANOS: La demanda en términos de almacenamiento y potencia computacional es predecible; por lo tanto, suponemos que no hay una diferencia significativa en el valor que podrían proporcionar los tres modelos de nube respecto a la gestión de la demanda y la escalabilidad.		
Parámetro: Fiabilidad del servicio: disponibilidad y rendimiento		
Requisito		
El servicio debe estar disponible el 99,9% del tiempo y el tiempo de inactividad no planificado debe ser inferior a 1 hora. Se requiere alta producción (*throughput*) y tiempo de espera reducido. PAE y APLICACIONES DE RECURSOS HUMANOS: El servicio debe estar disponible el 98% del tiempo y el tiempo de inactividad planificado y no planificado debe ser inferior a 4 horas. Se requiere alta producción (*throughput*) y tiempo de espera reducido. CORREO ELECTRÓNICO: El servicio debe estar disponible el 97% del tiempo y el tiempo de inactividad no planificado debe ser inferior a 2 horas. Se requiere producción (*throughput*) media y tiempo de espera reducido.		
Comunitaria	**Privada**	**Pública**
Una nube comunitaria podría ser inadecuada por la necesidad de gran replicación y rendimiento.	Una nube privada puede ofrecer gran replicación y rendimiento solo si la escala de la nube es suficientemente grande.	Elasticidad, resistencia, rentabilidad y total disponibilidad son los puntos fuertes de una nube pública de gran escala.
PAE, CORREO ELECTRÓNICO y APLICACIONES DE RECURSOS HUMANOS: Todas las soluciones propuestas pueden satisfacer la necesidad de disponibilidad media. Una nube pública es la solución que, como ya se mencionó varias veces en este informe, puede ofrecer la mayor disponibilidad. Las nubes privadas y comunitarias podrían ofrecer más rendimiento de servicio que una nube pública, debido a su cercanía a los usuarios finales. Una nube pública de gran escala normalmente ofrece distribución geográfica por defecto, pero concentra sus centros de datos en pocos Estados miembros.		
Parámetro: Continuidad del negocio		

Requisito		
HCE, PAE, CORREO ELECTRÓNICO y APLICACIONES DE RECURSOS HUMANOS: Los proveedores de estos sistemas deben aplicar planes de continuidad comercial y estar preparados para la recuperación ante desastres. HCE: Un plan de continuidad comercial debe tener en cuenta que cualquier tiempo de inactividad puede durar más de 1 hora. PAE y APLICACIONES DE RECURSOS HUMANOS: Un plan de continuidad comercial debe tener en cuenta que cualquier tiempo de inactividad puede durar más de 4 horas. CORREO ELECTRÓNICO: Un plan de continuidad comercial debe tener en cuenta que cualquier tiempo de inactividad puede durar más de 2 horas.		
Comunitaria	**Privada**	**Pública**
HCE: Una nube comunitaria es algo mejor (aunque similar) que una nube privada, a menos que se aplique en varias regiones y países. PAE: una nube comunitaria es algo mejor (aunque similar) que una nube privada, a menos que se aplique en varias regiones y países. La posibilidad de obtener mejores niveles de continuidad del negocio depende del número de entidades que se unan a la comunidad. Cuanto mayor es el número y la escala de las entidades (organismos públicos) que participan en la comunidad, mayor es la posibilidad de alcanzar un nivel de continuidad del negocio similar a los niveles que ofrecen las nubes públicas.	HCE (así como el resto de servicios): En una nube privada el grado de continuidad del negocio se reduce en comparación con una nube pública.	HCE: Una nube pública, que implementa un proveedor grande, puede distribuirse geográficamente. Cuando cumple la legislación sobre protección de los datos de salud en un determinado país, simplifica la continuidad del negocio. Una nube pública, que implementa un proveedor grande, puede distribuirse geográficamente. Si cumple los requisitos de auditoría, rendición de cuentas (*accountability*) y responsabilidad, así como la legislación sobre protección de datos de un país en concreto, simplifica la continuidad del negocio. CORREO ELECTRÓNICO: Una nube pública, que implementa un proveedor mayor, puede distribuirse geográficamente. Si cumple los requisitos de auditoría, rendición de cuentas (*accountability*) y responsabilidad, así como la legislación sobre protección de datos de un país en

		concreto, simplifica la continuidad del negocio.
Parámetro: Colaboración e interoperabilidad		
Requisito		
HCE: Potencialmente, todos los hospitales, clínicas, etc. en territorio nacional y en los Estados miembros de la Unión Europea podrían requerir acceso al servicio. PAE: Potencialmente, todas las administraciones públicas de cualquier nivel (local, regional y nacional) y los organismos que velan por el cumplimiento de las leyes podrían requerir acceso al servicio.		
Comunitaria	**Privada**	**Pública**
HCE, PAE y APLICACIONES DE RECURSOS HUMANOS: En una nube comunitaria, el nivel de interoperabilidad intracomunitario y extracomunitario se acuerda según las necesidades y requisitos de los miembros. Específico de PAE: Las autoridades locales necesitarían federar algunos servicios en una nube comunitaria, por lo que las autoridades locales tendrían que considerar la disponibilidad de cada nodo y la interoperabilidad. En una nube comunitaria, habría incluso que garantizar la consistencia de la identificación y la identificación de autoridades.	HCE, PAE y APLICACIONES DE RECURSOS HUMANOS: Las nubes privadas permiten a los usuarios utilizar ciertas configuraciones, aunque la interoperabilidad debe introducirse sobre o desde fuentes externas. Resulta más sencillo crear servicios auxiliares encima.	HCE, PAE y APLICACIONES DE RECURSOS HUMANOS: En una nube pública, la interoperabilidad es una propiedad intrínseca y puede permitir un enfoque sistemático.
Parámetro: Identidad, autenticación y gestión de acceso		
Requisito		
HCE: Las identidades de pacientes deben gestionarse internamente. El proceso de facilitar las credenciales y los permisos de los usuarios (pacientes, médicos, personal administrativo, etc.) debe gestionarse internamente. Se utiliza una combinación de RBAC y MAC. Los hospitales, clínicas, etc. suelen poseer datos. Los proveedores sanitarios definen las políticas de control de acceso según el consentimiento del paciente y de las políticas de la organización y nacionales. PAE, CORREO ELECTRÓNICO y APLICACIONES DE RECURSOS HUMANOS: Las identidades de los ciudadanos puede gestionarse internamente o mediante un proveedor externo o proveedor de nube. El proceso de facilitar las credenciales de los usuarios (ciudadanos, personal administrativo, etc.)		

puede gestionarse internamente o mediante un proveedor externo o proveedor de nube. Se requiere un sistema de control de acceso basado en roles para PAE y APLICACIONES DE RECURSOS HUMANOS.		
Comunitaria	**Privada**	**Pública**
HCE: En nubes privadas: • Existe control al acceso administrativo. • Es más fácil ofrecer acceso para datos de pacientes. • Es más fácil la gestión de identidades. • Resulta más simple la aplicación del MAC. PAE, CORREO ELECTRÓNICO y APLICACIONES DE RECURSOS HUMANOS: En nubes privadas y comunitarias, existe control sobre la identidad y sistemas de control de acceso para usuarios y administradores. Pueden utilizarse tarjetas inteligentes expedidas por las administraciones públicas. Las administraciones públicas pueden facilitar infraestructura de clave pública (PKI).		HCE: Un sistema de gestión de acceso complejo, resultante de una combinación de RBAC y MAC, es difícil de integrar y de aplicar en una nube pública. PAE y APLICACIONES DE RECURSOS HUMANOS: Un sistema de gestión de acceso complejo es difícil de integrar y de aplicar en una nube pública. El sistema español para gestionar identidades parece de especial interés a este respecto. De hecho, en España el nuevo carné de identidad (DNIe) incorpora un dispositivo para crear y verificar una firma electrónica. La verificación se realiza según dos sistemas formales para validar los certificados: La *Fábrica Nacional de Moneda y Timbre* del Ministerio de Industria, Turismo y Comercio y el Ministerio de la Presidencia. El sistema funciona para ciudadanos en los sectores público y privado y ahora las características técnicas son públicas para permitir distintos desarrollos. Además, la *Fábrica Nacional de Moneda y Timbre* sirve como infraestructura de clave pública (PKI) para administraciones públicas. La base jurídica del enfoque común para los sectores público y privado en el sistema español para gestionar identidades se encuentra en la ley 59/2003 española, que es una transposición de la Directiva 1999/93/CE de la UE sobre la firma electrónica. CORREO ELECTRÓNICO: Un sistema de gestión de acceso complejo es difícil de integrar y de aplicar en una nube pública, especialmente si se considera el modelo SaaS.

Parámetro: Cifrado		
Requisito		
HCE, PAE y APLICACIONES DE RECURSOS HUMANOS: El cifrado de datos en tránsito y en reposo es un requisito de seguridad. Debe ser posible gestionar la clave privada. CORREO ELECTRÓNICO: El cifrado de datos en tránsito y en reposo es un requisito de seguridad. Debido a la naturaleza de la aplicación, el intercambio de correo electrónico fuera del dominio o de la soberanía gubernamental se descifrará usando el remitente del mensaje, el destinatario y los *routers* en cuestión. Esto debe tenerse en cuenta durante la especificación del requisito de cifrado. Debe ser posible gestionar la clave privada.		
Comunitaria	**Privada**	**Pública**
HCE, PAE, CORREO ELECTRÓNICO y APLICACIONES DE RECURSOS HUMANOS: En las nubes privadas y comunitarias, los procesos de distribución y revocación de claves de cifrado son más fáciles de aplicar, así como los mecanismos de almacenamiento y protección de claves.		HCE, PAE, CORREO ELECTRÓNICO y APLICACIONES DE RECURSOS HUMANOS: Es difícil integrar un sistema de gestión de claves externo en una nube pública. Durante el procesamiento, puede ser necesario descifrar conjuntos de datos y, por lo tanto, exponer su contenido en una infraestructura pública potencialmente compartida por otros miles de abonados; por lo tanto, se requieren mecanismos robustos de aislamiento. Puede implementarse un análisis del tráfico aunque todos los datos estén cifrados.

Parámetro: Cumplimiento legal		
Requisito		
HCE, PAE, CORREO ELECTRÓNICO y APLICACIONES DE RECURSOS HUMANOS: Debe especificarse la ubicación de datos y la jurisdicción legal. La legislación de ciertos países impone un requisito: los datos no pueden salir del territorio nacional. Es necesaria la transparencia total frente a otros proveedores. Para garantizar la responsabilidad, se requieren registros admisibles en los juzgados.		
Comunitaria	**Privada**	**Pública**
En nubes comunitarias, el cumplimiento legal puede conseguirse fácilmente, debido a: • Los requisitos legales comunes de los miembros de la comunidad. • El control sobre la cadena de suministro de servicios.	Las nubes privadas permiten la máxima confianza en que puede conseguirse el cumplimiento legal.	En nubes públicas, conseguir el cumplimiento legal y normativo resulta difícil o incluso imposible debido a: • Jurisdicciones legales y ubicaciones de datos inciertas. • Derecho limitado a la

		auditoría.
Todas las alternativas de nubes pueden cumplir los requisitos de registros admisibles en los juzgados. Las nubes comunitarias y privadas pueden controlar mejor la recopilación (nivel de detalle) y retención de registros.		

5.4. Selección de la solución e identificación de amenazas y debilidades

Las limitaciones legales pueden requerir la retención de los datos sanitarios en un lugar físico concreto. En este caso, las nubes privadas y comunitarias son las mejores soluciones para implementar servicios de HCE (así como PAE, CORREO ELECTRÓNICO y APLICACIONES DE RECURSOS HUMANOS). Esto se debe a la capacidad de estos modelos de nube de ofrecer cumplimiento jurídico y normativo y control de los requisitos para altos niveles de confidencialidad e integridad. Es preferible una solución de nube comunitaria que aúne varias organizaciones sanitarias regionales, nacionales o internacionales frente a una nube comunitaria que combine la sanidad con otros sectores.

Aparte de las limitaciones legales, si el enfoque principal es ofrecer los beneficios sanitarios de un sistema de HCE, las nubes públicas de gran escala tienen el mejor potencial para cumplir los estrictos requisitos de disponibilidad y resistencia de un sistema de HCE a un coste razonable. Si se superan las dificultades de cumplimiento legal y normativo, se preferirán frente a las nubes privadas y comunitarias, a menos que las autoridades sanitarias puedan permitirse inversiones significativas en especialistas de seguridad y provisión en exceso de recursos.

Existen amenazas que hay que considerar al utilizar nubes gubernamentales privadas y comunitarias para servicios de HCE:

- Falta de masa crítica para la infraestructura.
- Ataques motivados políticamente.
- Filtraciones de HCE en un fallo irreversible que cubre un periodo muy largo de historial personal.
- La extrema sensibilidad de las reputaciones de gobiernos, administraciones y organismos públicos a la filtración de registros sanitarios y otras incidencias de seguridad, como el uso de infraestructura gubernamental para lanzar ataques maliciosos.
- Pérdida de integridad de datos.
- No disponibilidad de datos.
- Mala definición de requisitos y clasificación de activos.
- Términos y condiciones inadecuados en contratos con socios comerciales.
- Falta de control de la ejecución de contratos.
- Fallo de aislamiento (ver informe de 2009), con lo cual se abre la puerta a la filtración de información (control ilegal), así como a problemas operativos
- Gestión de identidades y sistemas de control de acceso inadecuados.

- Incumplimiento de normativas de protección de datos.

La lista anterior de amenazas obviamente debe integrarse en el resto de amenazas técnicas incluidas en el Anexo IV.

Para mitigar las amenazas mencionadas, las autoridades sanitarias deben tener en cuenta las medidas y controles de seguridad descritos en el capítulo 6.

Preparación de una solicitud de oferta

En este capítulo proponemos un conjunto de cuestiones de seguridad y resistencia que pueden utilizarse como guía al preparar una solicitud de oferta. Deben verse o bien como medidas de seguridad que hay que incluir en las especificaciones del contrato o bien como demandas que tiene que satisfacer un tercero. Además, debe utilizarse el mismo conjunto de preguntas para preparar el plan de mitigación en la fase de tratamiento de riesgos. Las cuestiones cubren solicitudes de oferta de servicio por parte de nubes públicas, proveedores de servicios independientes, proveedores de gestión de servicios de infraestructuras, servicios de seguridad y otros proveedores de gestión de servicios que con acceso privilegiado a infraestructuras y plataformas (por ejemplo, servicio de apoyo o servicio de asistencia técnica, gestión de capacidad, consultores, gestión de incidentes, etc.).

Además, aconsejamos aprovechar los controles incluidos en el marco de garantía orientado a la nube, como el *Information Assurance Framework* (Marco de Garantía de la Información) de ENISA y la *Controls Matrix* (Matriz de Control) de la CSA al preparar la solicitud de oferta de servicio o el plan de mitigación de riesgos.

Por último, sugerimos evaluar el potencial del proyecto *Common Assurance Maturity Model* (CAMM) (2), diseñado como marco para calificar y probar con transparencia la capacidad de una solución seleccionada para ofrecer garantía de la información en toda la cadena de suministro.

A. Preparación

- ¿Dispone de sistemas de gestión de seguridad de la información?

- ¿Cómo facilitará los certificados de auditoría y otros certificados necesarios?
- ¿Puede apoyar mi plan de clasificación de datos y servicios?
- ¿Qué facilidades de registro ofrece, cómo se garantiza la integridad de los registros y cómo se controla el acceso a estos?
- ¿Qué medidas de seguridad personal apoya?
- Muestre cómo cumple los requisitos gubernamentales para seleccionar y vetar a personal que tiene acceso a datos, infraestructura y gestión.
- ¿Cómo protege el acceso privilegiado?
- ¿Cómo se aíslan mis datos de los de otros clientes?
- ¿Cómo se controla y garantiza el acceso autorizado por los juzgados a mis datos?
- ¿Qué mecanismos admite para gestionar los derechos de acceso a los datos según los diferentes roles o usuarios?
- ¿Admite la autorización de varios jefes o varios niveles?
- ¿Cómo previene y detecta el aumento de privilegios y la unión de compartimientos?
- ¿Puede aplicar y garantizar la separación de deberes entre varias entidades gubernamentales?
- ¿Cómo se controla el acceso a los datos?
- ¿Qué distintos niveles de acceso se admiten y cómo se controlan en distintas categorías de usuarios y operadores?
- ¿Cómo se admiten los distintos tipos de credenciales de autenticación?
- ¿Se admite el acceso según roles, y qué resistencia tiene la gestión de roles?
- ¿Qué medios admite para facilitar datos específicos a raíz de citaciones judiciales o investigaciones de informática forense?
- ¿Cómo garantizará la separación de intereses entre servicios de clientes que pueden ser competidores?
- ¿Se ofrece al usuario final asesoramiento y herramientas apropiadas para facilitar el almacenamiento de información con distintos requisitos de seguridad, disponibilidad y cumplimiento?
- ¿Cómo garantiza que los tipos de datos se asocien con sus propietarios? [¿Políticas de seguridad multinivel?] ¿El sistema de gestión de acceso traduce adecuadamente la autorización de pares de clasificación (*clearance of classification pairs*) de las TIC tradicionales?
- ¿El proveedor ofrece separación de registros por usuario-cliente?
- ¿Cómo ofrecerá transparencia en acuerdos de subcontratación que establezcan y que tengan un efecto material en un acuerdo de nivel de servicio de las administraciones públicas con usted?
- ¿Cómo facilitará la coherencia de la política con la interoperación de servicios?

- ¿Cómo se garantizará la interconexión entre los sistemas y los servicios heredados y la infraestructura de nube?
- ¿Qué medidas de seguridad y control de acceso admite el sistema heredado?
- ¿Qué incumplimientos podrían producirse en la interconexión?
- ¿Cómo comprueba el proceso de contratación de hardware (especialmente para operaciones sensibles de las administraciones públicas)?

B. Prestación de servicios

- ¿Qué nivel de disponibilidad puede garantizar?
- ¿Qué nivel de disponibilidad de los distintos componentes existe en la solución y cómo afectan a la disponibilidad del servicio?
- ¿Qué mecanismos existen para garantizar la coherencia de los datos?
- ¿Qué medidas toma para garantizar que borra completamente los datos?
- ¿Qué medidas defensivas profundas admite para protegerse contra amenazas y vulnerabilidades desconocidas?
- ¿Qué proceso utiliza para mitigar alteraciones por aplicar cambios en la configuración y en el software?
- ¿Qué cambios de software y configuración de procesos de gestión realiza?
- ¿Cómo garantiza que su infraestructura y software estén libres de vulnerabilidades conocidas?
- ¿Cuál es su política y proceso de notificación de actualizaciones en el software de la plataforma que requieren la adaptación de aplicaciones de software del cliente?
- ¿Las categorías de cambios están claramente definidas?
- Solicite la notificación continua de categorías de cambio para realizar una evaluación y análisis de riesgos con la frecuencia necesaria.

C. Respuesta y recuperación

- ¿Con qué rapidez puede restaurarse el servicio tras una interrupción?
- ¿Cómo se recupera de un fallo permanente del proveedor de servicios en la nube?
- ¿Ha probado su plan de continuidad del negocio y recuperación ante desastres (BC/DR)?
- Si surge un incidente, ¿cuál es la política para notificarlo e informar del mismo?

D. Cumplimiento legal y normativo

- ¿Puede garantizar el cumplimiento de requisitos en la zona geográfica de los datos?
- Si se recibe una citación judicial de obtención de datos que entra en conflicto con la jurisdicción local, ¿cuáles son los medios para apelar?

- Diligencia debida reguladora. Por ejemplo: ¿se hacen algunas simulaciones para verificar el cumplimiento?
- ¿Puede garantizar el acceso a registros para demostrar quién ha accedido a qué datos y cuándo?
- ¿Cómo garantiza la integridad y el no repudio de registros?
- ¿Los términos propuestos de servicio expresan claramente quién es responsable de qué partes de la política de seguridad y en qué casos?
- ¿Cómo se aplica el principio de rendición de cuentas (*accountability*)?
- Suponga que existe una cláusula de protección de datos comerciales en la legislación de un Estado miembro de la UE sobre la protección de datos de ciudadanos. Debido a un incidente con un ciudadano extranjero, se abre una investigación. ¿Las autoridades del otro país tendrán acceso a los datos?
- ¿Cómo controlo el cumplimiento del contrato? ¿Cómo se mide el control en tiempo real del cumplimiento del acuerdo de nivel de servicios (como por ejemplo, *jitter*, tolerancia de carga, entrega?

Conclusiones y recomendaciones

A partir del análisis de los puntos fuertes, puntos débiles, oportunidades y amenazas sobre la seguridad y resistencia de los tres modelos de nube (comunitaria, privada y pública) realizado por ENISA con la ayuda del grupo de expertos, se llegó a las siguientes conclusiones:

- El modelo comercial de computación de la nube, por una parte, puede ofrecer a las administraciones públicas numerosos beneficios y mejoras en comparación con la provisión de TI actual, como:
    - Más disponibilidad y fiabilidad, ya que la agrupación de recursos simplifica el manejo y el enmascaramiento de fallos de hardware y de pérdida de rendimiento debido a picos de demanda.
    - Más seguridad, ya que muchos proveedores de servicios en la nube tienen más y mejor conocimiento especializado, gestión y control de la seguridad que empresas y organismos gubernamentales.
    - Más valor, ya que el modelo de nube ofrece economías de escala y servicios de nube que pueden cambiarse fácilmente como respuesta a las necesidades cambiantes de los organismos gubernamentales en cuanto a TI.

- Por otra parte, sigue mostrando debilidades y exposición a amenazas significativas que podrían socavar toda la explotación de los beneficios que podría ofrecer dicho modelo. Las debilidades y amenazas están vinculadas principalmente con la falta de gobernanza y control sobre operaciones de TI y el posible incumplimiento de leyes y normativas. Las leyes y normativas nacionales de los Estados miembros de la Unión Europea imponen actualmente ciertas restricciones al movimiento de datos fuera del territorio nacional; además, existe un problema para determinar la legislación aplicable (leyes reguladoras) cuando se almacenan y procesan datos fuera de la Unión Europea o por un proveedor de servicios que no es de la UE. Las cuestiones principales que debe abordar cada organización pública y, más en general, cada administración pública central de la UE son:
    - Si los actuales marcos legales pueden cambiarse para facilitar la comunicación, el tratamiento y el almacenamiento de datos fuera del territorio nacional sin exponer la seguridad y privacidad de ciudadanos y la economía y seguridad nacional a riesgos inaceptables.
    - En ese caso, si mover los datos de los ciudadanos fuera del territorio nacional es un riesgo que se puede asumir.

- Si la solución de compromiso entre los riesgos de perder control sobre los datos y los efectos beneficiosos de la distribución geográfica es positiva para ellos.

Estas consideraciones se aplican en general a todos los modelos de implementación de nube (es decir, pública, privada, comunitaria e híbrida), pero el impacto de las debilidades y amenazas varía según el entorno interno y externo concreto de las organizaciones públicas en los distintos Estados miembros y según el modelo de implementación y prestación considerado. En términos jurídicos y de gobernanza de datos, las nubes públicas, sin duda, representan la solución más arriesgada en comparación con nubes comunitarias y privadas, por los siguientes motivos:

- Los propietarios de nubes (proveedores de nubes públicas) y usuarios (organismos públicos) tienen distintas misiones e intereses, que a veces pueden entrar en conflicto.
- Empresas que no son de la UE pueden ser propietarias de nubes públicas.
- Los proveedores de nubes públicas ofrecen menos transparencia sobre sus medidas de seguridad y resistencia en comparación con otras opciones de nubes o TI interna.
- Los proveedores de nubes no están obligados a informar de incidencias de seguridad y resistencia. Aunque los usuarios pueden identificar las incidencias que tengan en la disponibilidad del servicio, no resulta fácil identificar incumplimientos de integridad, confidencialidad y protección de datos y su impacto. En cuanto a las nubes privadas y comunitarias, damos por sentado que el propietario de una nube privada y los miembros de una nube comunitaria tendrán una actitud más transparente a la hora de informar de incidencias a ciudadanos o usuarios y que, en el caso de una nube que opera un tercero, el contrato puede incluir una cláusula que obligue a notificar incidencias.

- La conectividad de internet es una base fundamental del modelo de nube; sin conectividad, obviamente, no es posible acceder a los servicios en nube. La calidad y el rendimiento de los servicios de comunicación (capacidad, latencia, etc.) muchas veces no son homogéneos en la Unión Europea y aún existen zonas (especialmente rurales) en varios Estados miembros donde la calidad del servicio es bastante deficiente.

- La falta de gobernanza y control, como se ha mencionado en el punto 2 de este apartado, parece ser una debilidad inherente al modelo de nube (especialmente respecto a las nubes públicas y el SaaS), aunque, como ya mencionó varias veces ENISA (por ejemplo, en el informe de 2009), la situación puede mejorarse consiguiendo transparencia en el mercado y negociando términos y condiciones apropiados en los contratos. Hay que señalar que el principio de transparencia (es decir, transparencia para los interesados) también se menciona en el borrador de la comunicación de la Comisión Europea "*A comprehensive approach on personal data protection in the European Union*" ("Una enfoque global de la protección de los datos personales en la Unión Europea") (19),

así como en el reciente discurso de la Comisaria Natalie Kroes sobre la computación en la nube y la protección de datos (25).

Al alcanzar un nivel adecuado de transparencia en términos de seguridad y requisitos de resistencia para organismos públicos y en términos de controles y prácticas de seguridad aplicados por los proveedores de la nube o de servicios, es posible combinar los requisitos de seguridad del cliente con los niveles de seguridad de servicio que se ofrecen. La reciente publicación del NIST "*Proposed Security Assessment and Authorization for U.S. Government Cloud Computing*" (26) y el proyecto CAMM (*Common Assurance Maturity Model*), en el que participa directamente ENISA, son explícitamente relevantes aquí.

- Para las aplicaciones sensibles, las nubes privadas y comunitarias parecen ser las soluciones que mejor encajan actualmente en las necesidades de las administraciones públicas, ya que ofrecen un mayor nivel de gobernanza, control y visibilidad, aunque, al planificar una nube comunitaria o privada, debe prestarse especial atención a la escala de la infraestructura, ya que no se conseguirán los beneficios de resistencia y seguridad del modelo de nube si no se alcanza la masa crítica necesaria de infraestructuras.

- La opción de nube pública ya puede proporcionar un servicio muy fiable con un nivel satisfactorio asociado de garantía de datos, siendo la más rentable. Además, la nube pública puede ofrecer el mayor nivel de disponibilidad del servicio, pero debido a la complejidad normativa actual de transferencia de datos transfronteriza, dentro y fuera de la UE, su adopción debe limitarse a aplicaciones no sensibles o no críticas y en el contexto de una estrategia definida para la adopción de la nube, que debe incluir una clara estrategia de salida. Al mismo tiempo, varias iniciativas emergentes, como la *CSA Guidance* (Directrices de la CSA) y otras dos iniciativas de la CSA, *Control Matrix* y *Consensus Assesment*, así como la labor del consorcio *Common Assurance Maturity Model* (CAMM) (2), están impulsando el criterio de referencia en cuanto a ofrecer una transparencia y garantía que permitan usar el modelo de la nube pública en aplicaciones más sensibles.

- Independientemente del modelo de implementación elegido, es evidente que solo puede conseguirse y mantenerse un nivel satisfactorio de seguridad y resistencia del servicio si:
    - Se identifican claramente los requisitos del servicio.
    - Se define claramente un nivel aceptable de servicio.
    - Se supervisa continuamente el cumplimiento de parámetros de seguridad y resistencia.
    - Existe coordinación entre la supervisión, la gestión de incidentes y los procesos de gestión de continuidad del negocio.

7.1 Recomendaciones a gobiernos, administraciones y organismos públicos

1. Se recomienda a las administraciones públicas adoptar un enfoque escalonado, con la capacidad de dar marcha atrás en cada etapa, dado que la complejidad del entorno de nube

introduce variables desconocidas que podrían ser muy difíciles de gestionar. Los gestores públicos de cualquier nivel deben considerar la interconexión y las interdependencias del sistema (la mayoría de las cuales pueden ser desconocidas), especialmente al trasladar simultáneamente varios servicios a un sistema de nube. Los gestores públicos deberán tener en cuenta esta cuestión en el contexto actual, en el que el entorno cambia de forma dinámica, y nuestros conocimientos sobre la vulnerabilidad y los mecanismos de ataque, así como la complejidad de los controles relacionados, son incompletos. Los gestores públicos no deberán dar por sentado que la implementación con éxito de una aplicación en un entorno de la nube supone, de forma automática, un indicio positivo que aconseje llevar a cabo muchas otras implementaciones, sino que deberán examinarse de forma detenida e individual los requisitos de seguridad y resistencia de cada aplicación y compararse con las arquitecturas de la nube y los controles de seguridad ya disponibles.

2. Las administraciones públicas nacionales deben elaborar una estrategia sobre computación en la nube que tenga en cuenta las implicaciones en cuanto a la seguridad y la resistencia que tendrán dichos modelos de suministro de servicios en el contexto de sus economías nacionales y servicios para los ciudadanos en los próximos 10 años. Quienes los adopten en primer lugar en cada Estado miembro podrán percibirse como posibles bancos de pruebas, aunque será esencial contar, al menos en el ámbito nacional, con un planteamiento coherente y armonizado respecto a la computación en la nube con el fin de evitar: 1) la proliferación de plataformas y formatos de datos incompatibles (ausencia de interoperabilidad de servicios), 2) un planteamiento incoherente respecto a la seguridad y la resistencia, incluido un planteamiento incoherente e ineficaz respecto a la gestión de riesgos y 3) la ausencia de masa crítica.

3. Recomendamos a las administraciones públicas que estudien el papel que desempeñará la computación en la nube en el contexto de la protección de las infraestructuras de la información crítica. No resulta descabellado pensar que la computación en la nube, en todas sus posibles implementaciones, prestará servicio, en un futuro cercano, a una parte significativa de ciudadanos, pequeñas y medianas empresas y administraciones públicas de la Unión Europea y, por tanto, las infraestructuras en la nube desde las que se prestan dichos servicios deberán disponer de protección. En otras palabras, las estrategias nacionales de computación en la nube deberán dirigirse a comprender y abordar, entre otras cuestiones, los efectos de la interoperabilidad e interdependencias de las nubes nacionales y supranacionales, así como a evaluar el impacto de posibles fallos en cascada, valorar la oportunidad de introducir un plan de informes de incidencias para proveedores de la nube similar al que ya se adoptó en el sector de telecomunicaciones (en concreto, nos referimos al mecanismo de generación de informes que introducen los artículos 4 y 13 de la recientemente adoptada Directiva 2009/140/CE[20]) y prepararse para posibles gestiones de crisis en caso de producirse incidentes a gran escala de esta índole.

[20] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0037:0069:EN:PDF

4. Recomendamos a las administraciones públicas nacionales y a las instituciones de la Unión Europea que continúen investigando el concepto de una nube gubernamental europea como un espacio virtual supranacional en el que pueda aplicarse un conjunto de normas coherente y armonizado, tanto en términos de legislación como de medidas de seguridad, en donde puedan promoverse la interoperabilidad y la estandarización. Además, una infraestructura de la Unión Europea de esta amplitud podría emplearse en el contexto de un plan de ayuda y asistencia mutuas paneuropeo para casos de emergencias.

Más concretamente, si los organismos públicos deciden finalmente pasarse a la computación en la nube, deben:

- Teniendo en cuenta la estrategia nacional, definir sus requisitos (posiblemente utilizando como ayuda los sugeridos en este informe) para identificar qué solución de nube se adapta a sus necesidades. Los gestores públicos deberán tener en cuenta también los factores humanos (tales como la concienciación sobre la seguridad y la resistencia, o la resistencia a los nuevos modelos de medidas de seguridad) y los marcos normativos.

- Para una buena gobernanza, establecer un proceso de gestión de seguridad de la información, que incluya gestión de riesgos, una política para la resistencia y seguridad de la información, gestión de activos (físicos y de información), etc., basándose en las buenas prácticas disponibles.

- Los gestores públicos deben centrarse en un catálogo de servicios generales y una clasificación de activos físicos y de información; para cada servicio y activo deben especificarse los requisitos apropiados de resistencia y seguridad. Sabemos que la mayoría de las grandes instituciones no podrán completar dicha tarea en un tiempo razonable, ya que somos conscientes de que en ciertos casos aún no tienen una imagen completa de sus activos. Una alternativa viable, en el contexto del enfoque escalonado hacia la computación en la nube, sería empezar con la definición de categorías macro de activos y servicios (por ejemplo, no sensibles y no críticos, de sensibilidad y criticidad media, etc.) y elaborar una clasificación detallada de activos según la lógica sencilla de que el primer servicio en migrar a la nube debe ser el primero en clasificarse (antes de la migración).

- Definir niveles aceptables de servicio (una referencia, por ejemplo, disponibilidad) para sus requisitos. Utilizarán las referencias para medir el rendimiento de sus servicios.

- Identificar el conjunto de controles y su grado de especificidad para alcanzar un nivel mínimo aceptable de garantía de datos y resistencia de servicios.

- Asegurarse de que todos los requisitos esenciales de seguridad, resistencia y jurídicos están detallados en sus requisitos de nivel de servicios y especificados en sus acuerdos de nivel de servicio. Éstos deben redactarse al planificar una migración de servicio. Por ejemplo, los

acuerdos de nivel de servicio deben incluir el derecho de auditar (o al menos el acceso a un informe de auditoría independiente), los medios para recuperar datos y aplicaciones (es decir, evitar el bloqueo) y detallar el nivel de supervisión y elaboración de informes, etc.

- Establecer un marco de medida (incluyendo indicadores principales de objetivos y rendimiento) para evaluar continuamente si se cumple lo siguiente:
    - Objetivo(s) de nivel de servicio.
    - Nivel de preparación y capacidad de prevención en caso de incidencias como fallos y ataques maliciosos.
    - Eficiencia y efectividad de la fase de reacción y recuperación tras un evento perjudicial.
- Tener en cuenta las normativas relevantes nacionales e internacionales que se aplican a terceros (por ejemplo, directivas de firma digital electrónica, garantías de terceros ISO) para garantizar la resistencia de las comunicaciones entre todas las partes implicadas en el suministro del servicio (administraciones públicas, ciudadanos, proveedores de servicios, grupos comerciales, así como los sistemas). Deben garantizarse la autenticidad de las identidades de las partes y su autorización para realizar una acción, el momento en el tiempo (es decir, sello de fecha y hora) y la ubicación.
- Aplicar, en los procesos de control de identidades y acceso, los principios de necesidad de saber, mínimo privilegio y separación de funciones.
- Tener herramientas, metodologías y estructuras de gobernanza para, p. ej., garantizar la diligencia debida.
- Comprobar la estabilidad financiera y solvencia de los socios comerciales, incluidas las líneas relevantes de negocios para evitar interrupciones inesperadas de los servicios o el bloqueo.
- Garantizar que se mantengan conexiones de telecomunicaciones, dependencias críticas (por ejemplo, electricidad), potencia de procesamiento y capacidad de almacenamiento de forma satisfactoria.
- Comprobar la prioridad de reanudación de comunicaciones de terceros y servicios de nube en caso de interrupciones.
- Probar el plan de continuidad del negocio a lo largo de toda la cadena de suministro de servicios.
- Para aplicaciones muy críticas, planificar ante la posible indisponibilidad del servicio de nube. Debe haber un mecanismo para permitir el acceso a servicios de TI incluso cuando no esté disponible la conexión a la(s) nube(s).

Por último, los proveedores de la nube y los proveedores de servicios independientes deberán considerar las recomendaciones que se incluyen en este informe como posible fuente de información a la hora de alinear sus ofertas comerciales y propuestas de valores con las necesidades y requisitos de los usuarios.

Glosario

AAC	Autenticación, autorización y contabilidad.
AC	Autoridad de certificación.
Activo	El objeto de la protección en un análisis de seguridad.
ANS	Acuerdo de nivel de servicio.
AP	Autoridad pública.
API (en su sigla en inglés)	Interfaz de programación de aplicaciones: especificación de un interfaz publicado por un proveedor de software.
Aplic.	En este informe se utiliza como abreviatura de aplicaciones.
ARP (en su sigla en inglés)	Protocolo de resolución de direcciones. (2)
ASL	Autoridad sanitaria local.
Ataque por canal lateral	Cualquier ataque basado en información obtenida a partir de la implementación física de un sistema. Por ejemplo, la información de tiempo, el consumo de energía, fugas electromagnéticas o incluso el sonido pueden proporcionar una fuente adicional de información que puede ser aprovechada para romper el sistema.
BS	*British Standard*.
BSDG	*Bundesdatenschutzgesetz*. (Ley de Protección de Datos alemana)
CC	Criterios comunes.
CEO (en su sigla en inglés)	Director ejecutivo.
CISO (en su sigla en inglés)	Director de Seguridad de la Información.
Citación judicial	En este contexto, orden de una autoridad legal para confiscar pruebas.
	Common Assurance Maturity Model.
Confidencialidad	Garantiza que la información está accesible únicamente al personal autorizado a acceder a dicha información (ISO 17799).
Co-residencia	Uso compartido de los recursos de hardware o software por los clientes de los servicios de la nube.
CPU (en su sigla en inglés)	Unidad de procesamiento central.
CRL (en su sigla en inglés)	Lista de certificados revocados.
CRM (en su sigla en inglés)	Gestión de la relación con los clientes.
CSO (en su sigla en inglés)	Director de Seguridad.
CTO (en su sigla en inglés)	Director de Tecnología.
DA	Directorio activo.
DAFO	Debilidades, amenazas, fortalezas y oportunidades.
DDoS (en su sigla en inglés)	Ataque distribuido de denegación de servicio.
Desprovisión	El proceso de aplicar la retirada del uso de un recurso, o de

	desautorizar su uso por un grupo de usuarios.
Disponibilidad	La proporción de tiempo durante la que un sistema puede realizar su función.
DNIe	Documento Nacional de Identidad Electrónico.
DPD	Directiva sobre Protección de Datos.
EDoS (en su sigla en inglés)	Denegación económica de sustentabilidad.
EEE	Espacio Económico Europeo.
Encargado del tratamiento de datos (*data processor*)	Persona física o jurídica, autoridad pública, agencia u otro organismo que procesa los datos personales en nombre del responsable del tratamiento de los datos.
Escrow	El almacenamiento de un recurso por un tercero que tiene acceso a dicho recurso cuando se satisfacen una serie de condiciones bien definidas.
Fiabilidad	Medida de la conformidad con la que un componente informático funciona de acuerdo a sus especificaciones.
FIM (en su sigla en inglés)	Gestión de identidades federadas.
Resistencia	La capacidad de un sistema de ofrecer y mantener un nivel aceptable de servicio en el supuesto de que se produzca un fallo (involuntario, intencionado u originado de forma natural).
Hipervisor	Plataforma de virtualización del software o hardware del equipo que permite utilizar, al mismo tiempo, diferentes sistemas operativos en un mismo equipo anfitrión.
HSM (en su sigla en inglés)	Módulo de Seguridad Hardware.
Https	Conexión Http mediante TLS o SSL.
IaaS (en su sigla en inglés)	Infraestructura como servicio (arquitectura de la nube).
IDS (en su sigla en inglés)	Sistema detector de intrusos.
Información clasificada	Información catalogada como confidencial por el sistema de clasificación de una administración pública o empresa. Un sistema de clasificación típico incluye varios niveles: *sin clasificar*, *restringida*, *confidencial*, *secreta* o *altamente confidencial*. La información clasificada corresponde típicamente al nivel de información "restringida" o a un nivel superior.
Integridad	La propiedad de que la información no ha sido modificada maliciosa o accidentalmente durante el almacenamiento o transmisión.
Interesado	Persona física identificada o identificable (véase la Directiva de la UE 95/46/CE) de la que se recopilan los datos y/o de la que se procesan los datos.
IP (en su sigla en inglés)	Protocolo de Internet.
IPS (en su sigla en inglés)	Sistema de protección ante intrusiones.
ISO (en su sigla en inglés)	*International Organization for Standardization* (Organización Internacional de Normalización).
ISV (en su sigla en inglés)	Proveedores independientes de software.

ITIL (en su sigla en inglés)	La Biblioteca de Infraestructura de Tecnologías de Información (ITIL) es un conjunto de conceptos y prácticas para la gestión de los servicios de la tecnología de la información (ITSM) y el desarrollo y las operaciones de la tecnología de la información.
Jitter	La variación en el tiempo en la llegada de los paquetes, causada por congestión de red, pérdida de sincronización o por las diferentes rutas seguidas.
LAN (en su sigla en inglés)	Red de área local.
Latencia	Es el tiempo necesario para que un paquete de información se transfiera de un lugar a otro.
LDAP (en su sigla en inglés)	Protocolo Ligero de Acceso a Directorios.
Linkability	La linkability describe la probabilidad de que un conjunto determinado de información permita establecer una identidad entre dos o más seudónimos.
LMS (en su sigla en inglés)	Sistema de gestión de permisos de trabajo.
MAC (2) (en su sigla en inglés)	*Mandatory Access Control*.
MAC (en su sigla en inglés)	*Media Access Control* (dirección de un nodo de red en IP).
MITM (en su sigla en inglés)	*Man in the Middle* (o intermediario, una forma de ataque).
Motor del servicio	El sistema responsable de ofrecer servicios de nube.
MSS (en su sigla en inglés)	Servicio de seguridad gestionada.
MV	Máquina virtual.
NIS (en su sigla en inglés)	Seguridad de red y de la Información.
NIST (en su sigla en inglés)	*National Institute of Standards and Technology (Estados Unidos)*.
No repudio	La prueba mediante la cual una parte en una controversia no puede repudiar o rechazar la validez de una declaración o contrato.
NRA (en su sigla en inglés)	Autoridad reguladora nacional (para telecomunicaciones).
Objetivo de seguridad	Documento en el que se especifican los criterios de evaluación de seguridad para corroborar lo declarado por un fabricante respecto a las propiedades de un producto (término utilizado en Criterios comunes).
OCSP (en su sigla en inglés)	Protocolo del estado del certificado en línea.
OTP (en su sigla en inglés)	Contraseña de un solo uso (tipo de autenticación).
OVF (en su sigla en inglés)	Formato de virtualización abierto.
PAE	Procedimiento administrativo electrónico.
Perfil de protección	Documento en el que se especifican los criterios de evaluación de seguridad para corroborar lo declarado por un fabricante respecto a una familia de productos de sistemas de información (término utilizado en Criterios comunes).
Perimetrización	Control de acceso a un activo o grupo de activos.
PN	Proveedor de la nube.
Port scan	Detección de los host de la red activos para ver qué puertos están abiertos y qué servicios ofrecen.

Producción (*Throughput*)	Cantidad de datos que son transmitidos en una dirección a través de un enlace dividido entre el tiempo que se tarda en transferirlos, generalmente expresado en bits o bytes por segundo.
Provisión	Proporcionar un recurso.
PSN	Proveedor de los servicios de la nube.
PVLAN	VLAN privada.
QoS (en su sigla en inglés)	Calidad de servicio.
RBAC (en su sigla en inglés)	Control de acceso basado en roles.
Red perimetral	En este contexto, una red de equipos que permite procesar y almacenar datos que entregará cerca de su destino final.
Responsable del tratamiento de datos (*data controller*)	Persona física o jurídica, autoridad pública, agencia u otro organismo que de forma independiente o conjunta con otros, determina el objeto y los medios mediante los que se procesan los datos personales; donde el objeto y los medios del procesamiento se determinen mediante leyes o normativas nacionales o comunitarias, el responsable del tratamiento o el criterio específico para esta nominación puede ser designado por las leyes nacionales o comunitarias.
ROI (en su sigla en inglés)	Retorno de la inversión.
ROSI (en su sigla en inglés)	Retorno de la inversión en seguridad informática.
RPO (en su sigla en inglés)	Objetivo de punto de recuperación.
RTO (en su sigla en inglés)	Objetivo de tiempo de recuperación.
RTSM (en su sigla en inglés)	Control de seguridad en tiempo real.
SaaS (en su sigla en inglés)	Software como servicio (arquitectura de la nube).
Sistema operativo anfitrión (*Host SO*)	El sistema operativo del proveedor de la nube, que opera múltiples sistemas operativos invitados.
Sistema operativo invitado (*Guest OS*)	Sistema operativo bajo control del cliente de la nube, que opera un entorno virtualizado.
SO	Sistema operativo.
SSL (en su sigla en inglés)	Protocolo de Capa de Conexión Segura (usado para cifrar el tráfico entre los servidores de la web y los navegadores).
SVA	Servicios de valor añadido.
TDU	Términos de uso.
TFUE	Tratado de funcionamiento de la Unión Europea.
TLS (en su sigla en inglés)	Seguridad de la Capa de Transporte (utilizado para cifrar el tráfico entre los servidores de la web y los navegadores).
Tolerancia	La capacidad de un *sistema* de responder adecuadamente a un fallo inesperado de hardware o software.
UPS (en su sigla en inglés)	Sistema de alimentación ininterrumpida.
VLAN (en su sigla en inglés)	Red de Área Local Virtual.
VPC (en su sigla en inglés)	Nube privada virtual.
VPN (en su sigla en inglés)	Red privada virtual.

Vulnerabilidad	Cualquier circunstancia o evento con potencial de tener un impacto negativo sobre un activo a través de un acceso no autorizado, destrucción, revelación, modificación de información, y/o denegación de servicio.
WAN (en su sigla en inglés)	Red de área amplia.
XML (en su sigla en inglés)	Lenguaje extensible de marcado.

Referencias

1. **Comisión Europea.** [En línea] 2010. http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/1602&format=HTML&aged=0&language=EN&guiLanguage=fr.

2. **CAMM - Common Assurance Maturity Model.** [En línea] http://common-assurance.com/.

3. **Diario Oficial de la Unión Europea.** [En línea] 2010. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0037:0069:EN:PDF.

4. **IDA.** [En línea] https://www.ida.gov.sg/News%20and%20Events/20050907165443.aspx?getPagetype=21.

5. **Etro, Federico.** [En línea] 2009. http://www.intertic.org/Policy%20Papers/RBE.pdf .

6. **Comisión Europea.** [En línea] 2010. http://europa.eu/press_room/pdf/complet_en_barroso___007_-_europe_2020_-_en_version.pdf.

7. **Declaración ministerial sobre la administración electrónica (Malmö, Suecia).** [En línea] 2009. http://www.tecnimap.es/userfiles/ministerial-declaration-on-egovernment.pdf.

8. **Comisión Europea.** [En línea] 2010. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52010DC0245%2801%29:EN:NOT.

9. **ENISA.** [En línea] 2007-2010. http://www.enisa.europa.eu/act/res/technologies/tech/tech.

10. **The Telegraph.** [En línea] 2010. http://www.telegraph.co.uk/technology/news/8186376/Cloud-computing-could-save-EU-economies-645bn-over-next-five-years.html.

11. **O'Reilly.** En línea] 2010. http://radar.oreilly.com/2010/06/randi-levin-on-cost-saving-thr.html.

12. **Wikipedia.** [En línea] http://en.wikipedia.org/wiki/Information_security.

13. **Office of Government Commerce.** ITIL - Service Operation. 2007.

14. **Instituto de Ingenieros Eléctricos y Electrónicos (IEEE).** [En línea] http://www.ieee.org/education_careers/education/standards/standards_glossary.html.

15. **ENISA.** [En línea] 2009. http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment.

16. **Grupo de Trabajo sobre Protección de Datos establecido en virtud del Artículo 29.** [En línea] 2010. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf.

17. **Consejo de Europa.** [En línea] 2010. http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079_reps_IF10_yvespoullet1b.pdf.

18. **Paolo, Balboni.** [En línea] 2010. http://common-assurance.com/wp-content/uploads/P_Balboni_Security-and-Privacy.

19. **Comisión Europea.** [En línea] 2010. http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf.

20. **NIST.** [En línea] http://csrc.nist.gov/groups/SNS/cloud-computing/.

21. **Comisión Europea.** [En línea] 2010. http://cordis.europa.eu/fp7/ict/ssai/docs/cloud-report-final.pdf.

22. **ISO.** [En línea] 2005.

23. **HIMSS.** [En línea] http://www.himss.org/content/files/EHRAttributes.pdf.

24. **Wikipedia.** [En línea] http://en.wikipedia.org/wiki/Human_resource_management_system.

25. **Kroes, Neelie.** [En línea] 2010. http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/10/686&format=HTML&aged=0&language=EN&guiLanguage=en.

26. **NIST.** [En línea] 2010. http://www.cio.gov/pages-nonnews.cfm/page/Federal-Risk-and-Authorization-Management-Program-FedRAMP.

27. **ENISA.** http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment. [En línea] 2009. http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment.

28. **Comisión Europea.** [En línea] 2010. http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/1602&format=HTML&aged=0&language=EN&guiLanguage=fr.

Anexo I – Análisis jurídico

Metodología

En los análisis jurídicos utilizamos la siguiente metodología.

PASO 1: En primer lugar, nuestro principal objetivo es responder a estas seis cuestiones fundamentales:

- ¿Qué servicios ("**Servicios**") identificados en la situación hipotética está considerando migrar a la nube la autoridad pública (AP)/gobierno?
- ¿Existe alguna ley o normativa específica que sea de aplicación a los Servicios y cuáles son las obligaciones o responsabilidades que corresponden a la AP/gobierno (p. ej., retención de los datos, protección de los datos, interoperabilidad, gestión de los expedientes médicos, revelación a las autoridades, etc.)?
- ¿Cuál es la naturaleza de los datos o información que se procesaría con estos Servicios?
- ¿Qué disposiciones legales en particular son de aplicación al tipo de datos o información que se procesará y cuáles son las obligaciones o responsabilidades que corresponden a la AP/gobierno (p. ej., protección de los datos, propiedad intelectual, confidencialidad, seguridad, etc.)?
- ¿Cómo es el flujo de los datos o información (interno[21] y externo[22]) durante el funcionamiento de estos Servicios?
- ¿Qué sujetos (personas físicas y/o jurídicas) participan en el funcionamiento de los Servicios y cuáles son sus roles (responsabilidades, deberes, obligaciones y compromisos)?

Estas preguntas se responderán respecto a cada situación particular tratada.
Tendremos en cuenta principalmente la legislación de la UE. Cuando la legislación o normativa pertinente no haya sido armonizada a nivel europeo, especificaremos los aspectos correspondientes y ofreceremos algunos ejemplos de las leyes en vigor en los Estados Miembros.

PASO 2: Una vez que se hayan respondido estas cuestiones, podremos:

- Confeccionar una lista de leyes y normativas que sean de aplicación, así como de las obligaciones y responsabilidades pertinentes de la administración pública/gobierno.
- Identificar las cuestiones legales y los riesgos legales asociados.

PASO 3: Posteriormente, analizaremos el impacto que tienen las cuestiones legales y los riesgos legales asociados en la migración de los Servicios a la nube por la AP/gobierno (y, de forma más general, por todas las partes implicadas). Más específicamente, identificaremos

[21] Dentro de la AP/gobierno
[22] De una AP/gobierno a otra AP/gobierno y/o de la AP/gobierno a los ciudadanos

los pros y los contras, así como los beneficios y los riesgos de migrar los Servicios a la nube. Respecto a los riesgos, propondremos la forma de tratarlos. Con el fin de mejorar la migración de los Servicios a la nube, finalizaremos ofreciendo una serie de recomendaciones sobre las soluciones y/o formas de hacer para las autoridades competentes.

Principales cuestiones normativas

Véase el párrafo 3.3.

Nube regional para la sanidad electrónica: situación núm. 1

Los servicios relacionados con la sanidad electrónica representan un sector en el que las administraciones públicas de los Estados miembros tienen que hacer frente a unos importantes retos. De hecho, por una parte debe ofrecerse una gran calidad y un alto rendimiento, mientras que por otra existe una presión cada vez mayor para reducir los gastos públicos. En otras palabras, es necesario poner en práctica el famoso dicho: "Haga más con menos": En este contexto, la introducción de nuevas tecnologías, nuevos modelos y servicios empresariales (por ejemplo, identificador de paciente único, historia clínica electrónica, archivo sanitario electrónico, programación en línea de citas para exámenes médicos, provisión en línea a los pacientes de los registros de revisión relacionados) puede solucionar estos desafíos.

La sanidad electrónica es un mercado en rápido crecimiento para los proveedores de servicios asociados a esta área. A través del Plan de Acción en Sanidad Electrónica, emitido en 2004, la Comisión Europea ha fomentado este crecimiento.[23] Además, debido al crecimiento en las oportunidades y demandas del mercado, el área de la sanidad electrónica ha sido seleccionada como parte de la iniciativa de mercados líderes.[24] En 2008, la Comisión de la UE emitió una recomendación sobre la interoperabilidad transfronteriza en los sistemas de historia clínica electrónica.[25] Esta recomendación prevé la “adopción de un marco legal global para la interoperabilidad de los sistemas de historia clínica electrónica. Este marco legal debe identificar y abordar la naturaleza confidencial de los datos personales relativos a la salud y ofrecer garantías específicas y adecuadas que amparen los derechos fundamentales relativos a la protección de los datos personales del individuo en cuestión." Además, anima a los Estados Miembros a “implementar la interoperabilidad de los sistemas de historia clínica

[23] *Comisión Europea, e-Health – making healthcare better for European citizens: An action plan for a European e-Health Area, Comunicación de la Comisión al Consejo, el Parlamento Europeo, el Comité Económico y Social Europeo y el Comité de las Regiones, COM(2004) 356 final, Bruselas, 30 de abril de 2004. Para más información sobre la estrategia de la Comisión sobre sanidad electrónica, véase ICT for Health y i2010: Transforming the European healthcare landscape: Towards a strategy for ICT for Health, Oficina de Publicaciones de la Unión Europea, Luxemburgo, 2006. El objetivo final es permitir el acceso a la historia clínica electrónica y a los datos de emergencia del paciente desde cualquier lugar de Europa. Véase también el Grupo de Trabajo establecido en virtud del Artículo 29 (WP 131/2007) el Documento de Trabajo sobre el tratamiento de datos personales relativos a la salud en las historias clínicas electrónicas; COM (2008) 414 Propuesta de Directiva del Parlamento y del Consejo Europeo relativa a la aplicación de los derechos de los pacientes en la asistencia sanitaria transfronteriza; COM(2008) 415 Marco Comunitario para la aplicación de los derechos de los pacientes en la asistencia sanitaria transfronteriza.*

[24] *Véase: <http://ec.europa.eu/information_society/activities/health/policy/lmi_ehealth/index_en.htm>.*

[25] *Véase: <http://ec.europa.eu/information_society/newsroom/cf/itemlongdetail.cfm?item_id=4224>.*

electrónica como parte integral de las estrategias regionales y nacionales de sanidad electrónica". La recomendación invita a los Estados Miembros a "comunicar anualmente a la Comisión las medidas adoptadas en relación con la implementación de la interoperabilidad transfronteriza de los sistemas de historia clínica electrónica."

El marco legal en el que se enmarcan los servicios sanitarios ofrecidos en Europa es bastante complejo. Los niveles de la atención sanitaria primaria y secundaria interactúan imponiendo deberes y obligaciones a todos los actores: administración pública, autoridades sanitarias locales, hospitales, consultas privadas, médicos, personal administrativo, etc. El marco legal no está armonizado en todos los Estados Miembros de la Unión Europea.[26] Esto se debe al hecho de que el sector sanitario es un dominio que sigue siendo en gran medida competencia de los Estados miembros. Antes de la promulgación del Tratado de Lisboa (1 de diciembre de 2009),[27] la Unión Europea (y, previamente, la Comunidad Europea) solo tenía un papel de apoyo y coordinación complementario en este sector (competencia complementaria paralela).[28] Podía utilizar instrumentos como las "resoluciones no obligatorias" (p. ej., las recomendaciones) para coordinar y fomentar acciones específicas en este campo, quedando excluidas explícitamente todas las medidas de armonización. El Tratado de Lisboa debería abrir una nueva fase en la armonización de la UE en este sector, clarificando y ampliando las competencias de la UE en la esfera del sector de la atención sanitaria pública. El Artículo 4.2 (k) (de la versión consolidada) del Tratado sobre el Funcionamiento de la Unión Europea[29] clasifica los "problemas de seguridad comunes en los asuntos de salud pública, para los aspectos definidos en este Tratado, como competencias compartidas entre los Estados Miembros y la Unión". Además, de acuerdo con el Artículo 6, la UE tiene una competencia complementaria paralela para la "protección y mejora de la salud humana". Se indican a continuación una serie de importantes intervenciones directas e indirectas de la UE en este campo:

- Marco legal europeo para los productos sanitarios[30];
- Directiva Europea relativa a la transparencia de las medidas que regulan la fijación de precios de los medicamentos para uso humano[31].
- Directiva Europea sobre el comercio electrónico[32], que contribuye al funcionamiento del mercado interno garantizando el movimiento libre de los servicios de la sociedad de la información, incluidos los servicios relativos a la salud sanitaria entre los Estados Miembros.

---

[26] *Véase el Study on the Legal Framework for Interoperable eHealth in Europe ("Estudio sobre el Marco Legal de la Salud electrónica Interoperable en Europa") de la Comisión Europea (2009), págs. 11 y siguientes, disponible en: <http://ec.europa.eu/information_society/activities/health/docs/studies/legal-fw-interop/ehealth-legal-fmwk-final-report.pdf>.*

[27] *http://www.consilium.europa.eu/showPage.aspx?id=1296&lang=en*

[28] *Véase, por ejemplo, Schutze, Co-operative federalism constitutionalised: the emergence of complementary competences in the EC legal order, European Law Review 2006, pág. 179.*

[29] *Disponible en: <http://eur-lex.europa.eu/JOHtml.do?uri=OJ:C:2010:083:SOM:EN:HTML>*

[30] *Disponible en: <http://ec.europa.eu/consumers/sectors/medical-devices/regulatory-framework/index_en.htm>*

[31] *Directiva 89/105/EEC; disponible en: <http://ec.europa.eu/enterprise/sectors/healthcare/competitiveness/pricing-reimbursement/transparency/index_en.htm>.*

[32] *La directiva 2000/31/CE establece los requisitos relativos a la información impuestos a los proveedores de servicios en la sociedad de la información, las normas que rigen las comunicaciones comerciales, las normas que rigen los contratos formalizados electrónicamente y la responsabilidad de los proveedores de servicios intermediarios. Disponible en: <http://ec.europa.eu/internal_market/e-commerce/directive_en.htm>.*

- Legislación de la UE sobre el libre movimiento de profesionales, incluidos profesionales sanitarios[33].
- Marco regulativo europeo para la protección de datos personales[34] y para la protección de la privacidad en las comunicaciones electrónicas[35].

En junio de 2008, la Comisión publicó una propuesta de directiva sobre los derechos de los pacientes en la atención sanitaria transfronteriza[36]. Conviene destacar que el artículo 16 se relaciona específicamente con la sanidad electrónica y prevé la adopción de "medidas específicas para lograr la interoperabilidad de los sistemas de tecnología de la información y la comunicación en el campo de la atención sanitaria, aplicables siempre que los Estados miembros decidan introducirlas. Estas medidas reflejarán las novedades que se produzcan en las tecnologías de la salud y en las ciencias médicas, y respetarán el derecho fundamental a la protección de los datos personales, de conformidad con la ley aplicable. En particular, especificarán las normas y terminologías necesarias para la interoperabilidad de los sistemas de tecnología de la información y la comunicación con el fin de garantizar la provisión de servicios de salud transfronterizos seguros, de alta calidad y efectivos. Asimismo, debe mencionarse que el artículo 14 propuesto solicita a la Comisión la "adopción de medidas que permitan a un farmacéutico o a otro profesional de la salud comprobar la autenticidad de una receta y si ésta ha sido emitida en otro Estado miembro por una persona autorizada, para lo que se desarrollará una plantilla de recetas comunitarias y se apoyará la interoperabilidad de las recetas electrónicas.

Situación hipotética

Para llevar a cabo un análisis exhaustivo de las cuestiones, y dada la falta de armonización en el sector de la sanidad electrónica en los Estados miembros, se ha diseñado una situación hipotética a escala local. A tal efecto, se ha considerado el hecho de que diversas autoridades sanitarias locales (ASL) italianas estén contemplando formalizar acuerdos conjuntos con una empresa nacional de telecomunicaciones para crear su propia nube. Dichas autoridades prevén migrar a la nube servicios como la historia clínica electrónica, el archivo sanitario electrónico, programación en línea de citas para exámenes médicos, provisión en línea a los pacientes de los registros de revisión relacionados y otros servicios de menor importancia, como los servicios administrativos (*back-end*), recursos humanos, nóminas y aprendizaje electrónico.

Los principales puntos que se deben investigar son la disponibilidad de servicios y datos, la autenticidad de los datos, la integridad, la aplicación de una seguridad fiable de la información, la

[33] *La directiva 2005/36/CE tiene por objeto garantizar que los Estados miembros promulguen normas uniformes, transparentes y no discriminatorias que reconozcan las cualificaciones profesionales y la experiencia para trabajar temporal o permanentemente en la Unión Europea; disponible en: <http://ec.europa.eu/internal_market/qualifications/future_en.htm>.*

[34] *Directiva 95/46/CE - Directiva sobre la Privacidad y la Protección de Datos, http://ec.europa.eu/justice/policies/privacy/index_en.htm*

[35] *Directiva 2002/58/CE - Directiva sobre la Privacidad y las Comunicaciones Electrónicas, http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&numdoc=32002L0058&model=guichett&lg=en*

[36] *Comisión Europea, Propuesta de Directiva del Parlamento y del Consejo Europeo relativa a la aplicación de los derechos de los pacientes en la asistencia sanitaria transfronteriza, COM(2008)414 final, http://ec.europa.eu/health/ph_overview/co_operation/healthcare/docs/COM_en.pdf*

resistencia de los servicios, la protección de datos personales y la adherencia a los requisitos legales (en especial en lo que respecta a la legislación sobre protección de datos).

Tipos de datos y flujo de datos entre las personas implicadas

Tanto la historia clínica electrónica (HCE) como el archivo sanitario electrónico (ASE) contienen información sobre la salud de una persona relativa a episodios clínicos pasados y presentes (por ejemplo, observaciones médicas, historial de hospitalización y cuidados de emergencia) con el fin de documentar el historial médico de la persona en cuestión. Los datos personales se interrelacionan empleando diversas herramientas informáticas, que en cualquier caso permiten a los diversos profesionales de la salud y organismos que hayan facilitado cuidados médicos a esa persona en algún momento recuperar y buscar fácilmente los datos.

Más en concreto, el archivo sanitario electrónico (ASE) es un archivo creado por un organismo de atención sanitaria que actúa como el responsable único del tratamiento de los datos (por ejemplo, un hospital o una residencia), en el que trabajan varios profesionales de la salud. Por el contrario, la historia clínica electrónica es un archivo creado por la agrupación de datos procedentes de diferentes responsables del tratamiento de los datos que, por regla general (aunque no es siempre el caso), operan dentro de la misma zona geográfica (p. ej., una unidad de atención médica y un laboratorio privado que operan en la misma región o área). Los archivos sanitarios, por ejemplo, también pueden estar constituidos por el conjunto de informes de salud en poder de los responsables de datos individuales que participan en una iniciativa de HCE a nivel regional. En consecuencia, la historia clínica electrónica y el archivo sanitario electrónico están íntimamente interrelacionados.

"Programación en línea de las citas para exámenes médicos" indica que los pacientes pueden formalizar citas interactuando con el sistema de reservas en línea de la autoridad sanitaria local.

"Acceso en línea a registros de revisión" significa que el paciente puede acceder a un "registro de revisión" en línea; en este caso "registro de revisión" es el registro escrito elaborado por un médico sobre el estado clínico del paciente tras una revisión clínica y/o los resultados de la prueba. En algunos casos, también permite descargar las "observaciones", es decir, los resultados de la revisión médica o de una prueba realizada al paciente, como una radiografía, una ecografía o un análisis de sangre, junto con el registro de revisión elaborado por el médico.

Todos los servicios que las autoridades sanitarias locales piensan migrar a la nube entrañan el procesamiento, no solo de datos personales, sino también de datos confidenciales (categoría especial de datos sobre salud, véase el artículo 8 de la Directiva 95/46/CE) por parte de diferentes responsables y encargados del tratamiento de datos, salvo en el caso de servicios administrativos (*back-end*), nómina y aprendizaje electrónico, por ejemplo, donde se procesan datos personales, pero es menos probable que se procesen datos confidenciales. Durante el funcionamiento de estos servicios, fluyen datos e información internos[37] y externos[38]. En ellos participan diversas personas con distintos roles en cuanto a la protección de datos, que además transfieren datos entre sí.

[37] *Dentro de la autoridad pública o el gobierno.*

Cuestiones legales

En términos generales, las normas que rigen las historias clínicas electrónicas, los archivos sanitarios electrónicos, la programación en línea de citas para exámenes médicos y la provisión a los pacientes de registros de revisión en línea relacionados se recogen en la legislación sobre sanidad de los Estados miembros, en la legislación sobre los derechos de los pacientes[39] y en las normativas sobre protección de datos, donde se especifican normas sobre cómo deben guardar y compartir las historias clínicas los proveedores, así como su contenido, archivado y derecho de acceso para los pacientes, etc.[40]
El presente análisis se centrará en la protección de datos y, desde un punto de vista más general, en el cumplimiento de los requisitos legales. Como punto de referencia, se tomarán las normativas europeas e italianas sobre esta materia. Es de esperar que el razonamiento general y las conclusiones se puedan aplicar a la mayoría de los Estados miembros. Nuestro objetivo es señalar cuestiones de importancia para la situación seleccionada y ofrecer un método de análisis que se pueda utilizar para evaluaciones en otros Estados miembros.

Sin duda, la legislación más importante es la relativa a la protección de datos. En concreto, la Autoridad Italiana de Protección de Datos emitió directrices sobre la provisión de historias clínicas electrónicas, archivos sanitarios electrónicos[41] y registros de revisión en línea.[42] Si desean consultar un análisis de cuestiones relativas a la "soberanía gubernamental y el control de la información y los datos", "adquisiciones del sector público"', "negligencia profesional de los proveedores de servicios en la nube" y "subcontratación de servicios en la nube y cambio de control de proveedor de servicios en la nube", les remitimos al apartado "Principales cuestiones normativas", ya que se trata de cuestiones generales (y no son específicas de la presente situación). Otras cuestiones, como "protección y seguridad de los datos", "interoperabilidad / transferencia al origen / cautividad del mercado", se

---

[38] *De una autoridad sanitaria local a otra autoridad sanitaria local y de la autoridad sanitaria local a los ciudadanos.*
[39] *Véase también la Carta Europea de Derechos de los Pacientes (2002); disponible en: <www.patienttalk.info/european_charter.pdf>.*
[40] *"En diversos Estados miembros, se ha delegado a las regiones la responsabilidad de importantes áreas del sistema de atención sanitaria. Sin embargo, esta descentralización se ha llevado a cabo de distintas formas y en diverso grado. […] Los gobiernos regionales italianos, a través de sus departamentos sanitarios, son los responsables de cumplir a nivel regional los principales objetivos nacionales del Plan Nacional de Salud. Los departamentos regionales de salud deben garantizar las prestaciones a la población por medio de una red de unidades sanitarias locales y de hospitales públicos y privados. Son responsables de funciones legislativas y administrativas, de planificar actividades de cuidados de salud, de organizar los suministros de conformidad con las necesidades de la población y de supervisar la calidad, la idoneidad y la eficacia de los servicios prestados. Las regiones tienen funciones legislativas y ejecutivas, así como funciones de asistencia técnica y de evaluación. Comisión Europea (2009) Study on the Legal Framework for Interoperable eHealth in Europe ("Estudio sobre el Marco Legal de la Salud electrónica Interoperable en Europa"), pág. 21; para ver cómo se ha aplicado la descentralización en diversos Estados miembros, consulte las páginas 21-24; véanse también las páginas 18 y 75 y siguientes; disponible en: <http://ec.europa.eu/information_society/activities/health/docs/studies/legal-fw-interop/ehealth-legal-fmwk-final-report.pdf>.*
[41] *Autoridad Italiana de Protección de Datos (2009) Guidelines on the Electronic Health Record and the Health File (publicado en la Gaceta Oficial de Italia, núm 178, con fecha de 3 de agosto de 2009); disponible en: <http://www.garanteprivacy.it/garante/doc.jsp?ID=1672821>.*
[42] *Italian Data Protection Authority (2009) Guidelines on Online Examination Records (documento adoptado el 25 de junio de 2009 y presentado a consulta pública de conformidad con la nota publicada en la Gaceta Oficial de Italia, núm 162, del 15 de julio de 2009); disponible en: <http://www.garanteprivacy.it/garante/doc.jsp?ID=1634292>.*

abordarán en la medida en que tengan relación con la situación planteada ahora. Para otros asuntos, les remitimos al apartado ya citado, "Principales cuestiones normativas".

Protección de los datos y seguridad de los datos

En este apartado abordaremos solo cuestiones muy concretas relativas a la presente situación, y presentaremos una introducción a cuestiones generales de protección y seguridad de los datos.

Transferencia

El Grupo de Trabajo del Artículo 29, en el Documento de Trabajo (WP 131/2007) sobre el tratamiento de datos personales relativos a la salud en las historias clínicas electrónicas (HCE), ha subrayado que "Teniendo en cuenta el elevado riesgo que existe para los datos personales contenidos en un sistema de HCE en un medio sin protección adecuada, […] todo tratamiento (sobre todo, el almacenamiento) de datos de las HCE deberá realizarse en jurisdicciones que apliquen la Directiva sobre protección de datos de la UE o un marco jurídico adecuado de protección de datos".[43] Además, a menos que el interesado o paciente haya dado su consentimiento explícito (obligatoriamente por escrito en diversos Estados miembros, si se trata de datos confidenciales) los datos personales de la HCE "deben transferirse a países que no formen parte de la Unión Europea o del Espacio Económico Europeo de forma anónima o, al menos, utilizando pseudónimos".[44]

Seguridad de datos

Debe implantarse un alto nivel adecuado de seguridad de datos para favorecer el rendimiento total del sistema (artículo 17 de la Directiva 95/46/CE).

Gestión de identidades, control de acceso e integridad de datos

Más concretamente, para que un sistema sea aceptable desde el punto de vista de la protección de datos, debe evitarse, de forma que sea casi imposible, el acceso de personas no autorizadas. Al mismo tiempo, la disponibilidad del sistema para profesionales autorizados debe ser casi ilimitada, si la necesidad de saber es genuina. Esto es lo que el Grupo de Trabajo del Artículo 29 recomienda en el documento WP 131/2007.[45] Además, "el marco jurídico por el que se crea un sistema de HCE debería prever la aplicación de una serie de medidas técnicas y organizativas adecuadas destinadas a evitar la pérdida de datos o la alteración, tratamiento y acceso no autorizados a los datos en el sistema de HCE". "La integridad del sistema debe garantizarse haciendo uso de los conocimientos e instrumentos

---

[43] *Grupo de Trabajo del Artículo 29, en el Documento de Trabajo (WP 131/2007) sobre el tratamiento de datos personales relativos a la salud en las historias clínicas electrónicas, pág. 19; disponible en: <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp131_en.pdf>.*

[44] Id

[45] *Grupo de Trabajo del Artículo 29, en el Documento de Trabajo (WP 131/2007) sobre el tratamiento de datos personales relativos a la salud en las historias clínicas electrónicas, pág. 19; disponible en: <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp131_en.pdf>.*

más avanzados en materia de informática y tecnología de la información".[46] El Grupo de Trabajo señaló también que el cifrado no debe usarse solo para la transferencia, sino también para el almacenamiento de datos en sistemas HCE.[47]

Como conclusión, el marco jurídico relativo a las medidas de seguridad debe prever especialmente la necesidad de:

- Desarrollar un sistema fiable y efectivo de identificación y autenticación electrónica, así como registros actualizados de manera constante, para comprobar la autorización de personas con acceso o que soliciten acceso al sistema de HCE.
- Registro y documentación exhaustivos de todos los pasos de procesamiento que hayan tenido lugar dentro del sistema, en especial, solicitudes de acceso de lectura o escritura, combinadas con comprobaciones internas periódicas y seguimiento de las autorizaciones.
- Mecanismos efectivos de copia de seguridad y recuperación para garantizar el contenido del sistema.
- Impedir el acceso no autorizado o la alteración de los datos HCE en el momento de la transferencia o del almacenamiento de copias de seguridad, por ejemplo, utilizando algoritmos criptográficos;
- Instrucciones claras y documentadas a todo el personal autorizado sobre cómo utilizar correctamente los sistemas de HCE y cómo evitar riesgos y violaciones de la seguridad.
- Una clara distinción de funciones y competencias en relación con las categorías de personas a cargo del sistema o, al menos, implicadas en el sistema, con previsión de responsabilidades en caso de deficiencias.
- Auditorías de seguridad periódicas, tanto internas como externas[48].

Todos estos requisitos de seguridad tan estrictos deben respetarse constantemente en el entorno de la nube, al margen de que el proveedor sea considerado responsable o encargado del tratamiento de los datos. De hecho, la obligación de implantar o garantizar un elevado grado de seguridad de datos recae sobre el responsable del tratamiento de los datos, que la transferirá al encargado del tratamiento de los datos por medio de un contrato o de una carta de nombramiento (artículo 17.2, 3 y 4).

A continuación, presentamos algunos ejemplos de disposiciones específicas relativas a medidas de seguridad tal y como se establecen en *Guidelines on the Electronic Health Record and the Health File* (G_EHR) o en *Guidelines on Online Examination Records* (G_OER), de la Autoridad Italiana de Protección de Datos, que prevé una gestión rigurosa de la identidad, el control de datos y la integridad de datos.

Deber/Obligación	Fuente

[46] *Id, pág. 19*
[47] *Id*
[48] *Id, págs. 19-20*

Deber/Obligación	Fuente
Dada la confidencialidad de los datos procesados mediante una historia clínica electrónica/archivo sanitario electrónico, deben formalizarse acuerdos técnicos específicos para garantizar un nivel apropiado de seguridad (apartado 31 del Código de Seguridad de Datos), sin perjuicio de las medidas mínimas que los responsables del tratamiento de los datos deben tomar en cualquier caso, de conformidad con el Código (sección 33 y siguientes). Si se utilizan sistemas de almacenamiento o archivado, deben llevarse a cabo las operaciones adecuadas para proteger los datos contra el uso no autorizado, el robo o la pérdida total o parcial del soporte de almacenamiento o de los dispositivos de procesamiento fijos o portátiles; para este fin, deben aplicarse tecnologías de cifrado a los sistemas de archivo o las bases de datos, o bien aplicar otras medidas de protección para impedir que los datos sean comprensibles para entidades no autorizadas. Deben tomarse también las siguientes medidas: • Deben aplicarse sistemas adecuados de autenticación y autorización a las personas a cargo del procesamiento, en relación con sus respectivos requisitos de procesamiento y acceso (por ejemplo, para buscar, cambiar y añadir registros). • Deben implantarse procedimientos para comprobar periódicamente la calidad y la uniformidad de las credenciales de autenticación y los perfiles de autorización que se aplican a las personas a cargo del procesamiento. • Deben especificarse criterios para cifrar o mantener separados los datos que pudieran revelar la salud o la vida sexual de otros datos personales. • Deben registrarse los accesos y las operaciones. • Debe implantarse un registro de auditoría para controlar los accesos a la base de datos y detectar anomalías. Como en el caso de las HCE, deben desplegarse protocolos de comunicación segura, aplicando normas de cifrado para comunicaciones electrónicas de datos entre los diversos responsables del tratamiento de los datos.	Parte II Sección 10 (G_EHR)
La naturaleza altamente confidencial de los datos personales que se procesan en relación con el acceso en línea a los registros de revisión requiere que se establezcan disposiciones técnicas específicas para garantizar un nivel de seguridad adecuado, como establece la sección 31 del Código, sin prejuicio de las medidas mínimas que se exigen de cada	Sección 6 (G_OER)

Deber/Obligación	Fuente
responsable del tratamiento de los datos en virtud del Código (véase la sección 33 y siguientes), y en especial las establecidas en la Regla 24 de las Especificaciones Técnicas a las medidas mínimas de seguridad (Anexo B del Código), por las que la transferencia de datos que puedan revelar la identidad genética de un individuo solo se permite en formato cifrado. Consulta en línea de registros de revisión por medio de servicios web en Internet Si el servicio que se va a facilitar consiste en permitir que un interesado acceda al sitio web del organismo de atención sanitaria que ha llevado a cabo la revisión en cuestión con el fin de descargar el respectivo registro, deben tomarse precauciones específicas, como las siguientes: • Protocolos de comunicación segura, basados en normas de cifrado para transferencias electrónicas de datos, incluidos certificados digitales de los sistemas que proporcionan servicios de red (protocolos http SSL - Capa de Conexión Segura). • Disposiciones adecuadas para prevenir que se adquiera la información contenida en el registro electrónico, si este se almacena en sistemas caché locales o centralizados después de haber sido consultado en línea. • Sistemas de autenticación adecuados basados en credenciales estándar o, preferiblemente, en sólidos procedimientos de autenticación. • Disponibilidad a corto plazo (máximo 45 días) del registro de revisión en línea. • Posibilidad de que el usuario impida la visualización en línea de los registros de revisión correspondientes o de que borre dichos registros, en parte o por completo, del sistema de acceso en línea. Envío por correo electrónico de los registros de revisión Si el responsable del tratamiento de los datos piensa enviar una copia de los registros de revisión a la dirección de correo electrónico del interesado, de conformidad con una solicitud concreta de éste, deberán tomarse las siguientes precauciones con respecto a los registros digitales: • Los registros de revisión deberán enviarse en forma de datos adjuntos al mensaje de correo electrónico, y no como texto incrustado en el cuerpo del mensaje. • Deberá protegerse el archivo el registro o registros de revisión para evitar la adquisición ilícita o no deseada de información por	

Deber/Obligación	Fuente
entidades diferentes al destinatario en cuestión. Para este fin, debe protegerse mediante contraseña el archivo, o aplicarse una clave de cifrado, que se notificará a los interesados por canales de comunicación diferentes (véase la Regla 24 de las Especificaciones Técnicas, anexo B al Código). Este requisito puede incumplirse si el interesado así lo solicita, tras haber sido debidamente informado, dado que el envío de registros de revisión a la dirección de correo electrónico especificada por el interesado no da lugar a una transferencia de datos médicos entre dos responsables del tratamiento de los datos, y consiste realmente en una comunicación de datos entre el proveedor de atención sanitaria y el interesado, a instancias del interesado. • Las direcciones de correo electrónico deberán ser validadas por medio de un procedimiento de control en línea *ad hoc* para evitar el envío de documentos electrónicos (aunque estén protegidos mediante cifrado) a otros destinatarios distintos al usuario concreto que los haya solicitado. Deberán aplicarse en todos los casos las siguientes medidas para procesar datos con el fin de facilitar estos servicios en línea a los usuarios: 1. Deberán implantarse sistemas de autenticación y autorización a las personas a cargo del procesamiento, en función de sus respectivos roles y requisitos de acceso y procesamiento (considerando, por ejemplo, si pueden buscar, modificar o completar la información); deberá aplicarse una sólida autenticación biométrica si los datos procesados pueden revelar la identidad genética de una persona. 2. Los datos que puedan revelar la salud y la vida sexual deberán mantenerse separados física y lógicamente de otros datos personales, procesados para fines administrativos o contables. Es más, el responsable del tratamiento de los datos debe diseñar procedimientos *ad-hoc* para desactivar inmediatamente la consulta en línea o interrumpir el envío por correo electrónico de registros de revisión relacionados con una persona que haya notificado el robo o la pérdida de sus credenciales de autenticación, o en cualquier otra circunstancia que pueda poner en peligro la confidencialidad de sus datos personales. En cualquier caso, deben aplicarse todas las medidas de seguridad necesarias para cumplir la prohibición de divulgar datos médicos establecidas en el Código (véanse las secciones 22.8 y 26.5 del Código).	

Derecho del paciente o interesado

Como se mencionó en la introducción, el responsable del tratamiento de los datos tiene la obligación de garantizar el derecho de acceso del interesado a los datos, como se describe en el artículo 12 de la Directiva 95/46/CE. Sin embargo, cuando se procesan datos personales relativos a la salud, las restricciones al derecho de acceso del paciente o interesado deben combinarse con los derechos específicos de acceso a registros de salud, establecidos en disposiciones nacionales sobre los derechos del paciente. En este caso concreto, no sólo se ha aplicado de forma poco uniforme la Directiva 95/46/CE, sino que los derechos de los pacientes se han definido y aplicado también de forma diferente según las diversas legislaciones nacionales.

Interoperabilidad / Transferencia al origen / "Cautividad del mercado"

La interoperabilidad de los sistemas de historia clínica electrónica (HCE) es una condición necesaria establecida tanto en la Recomendación de 2008 de la Comisión Europea sobre la interoperabilidad transfronteriza en los sistemas de historia clínica electrónica [49]como en la como en la Propuesta de directiva de 2008 de la Comisión Europea sobre los derechos de los pacientes en los cuidados de salud transfronterizos.[50]

La transferencia al origen y la cautividad del vendedor deben tenerse en cuenta en el sector de la sanidad electrónica, ya que representan graves amenazas para la continuidad del servicio. De hecho, la no disponibilidad (temporal) o la ineficacia de los servicios supondrá una considerable responsabilidad para los proveedores de sanidad electrónica (es decir, para las autoridades sanitarias locales, en este caso).

Consideraciones finales

Las principales cuestiones relativas a la migración de los servicios en la nube, como las historias clínicas electrónicas (HCE), los archivos sanitarios electrónicos (ASE), la programación en línea de citas para exámenes médicos y provisión en línea a los pacientes de los registros de revisión relacionados, deben identificarse en:

(i) La transferencia de datos del paciente.
(ii) La seguridad de datos del paciente.
(iii) La interoperabilidad.

La migración a la nube de servicios como la HCE, el ASE, la programación en línea de citas para exámenes médicos y la provisión en línea a los pacientes de los registros de revisión relacionados, puede ofrecer seguridad y ventajas de interoperabilidad. De hecho, es muy probable que un sólido proveedor de servicios en la nube tenga personal más competente y cualificado y mayores recursos económicos que cualquier autoridad sanitaria local, lo que permitirá a dichos proveedores garantizar

[49] *Véase: <http://ec.europa.eu/information_society/newsroom/cf/itemlongdetail.cfm?item_id=4224>.*
[50] *Comisión Europea, Proposal for a Directive of the European Parliament and the Council on the application of patients' rights in cross-border healthcare, COM(2008)414 final; http://ec.europa.eu/health/ph_overview/co_operation/healthcare/docs/COM_en.pdf*

estándares de seguridad del más alto nivel y promover la interoperabilidad global de esos servicios. Sin embargo, puede ser extremadamente difícil que los proveedores de servicios en la nube ofrezcan servicios que cumplan todos los exigentes, y a menudo no armonizados, requisitos regulativos mencionados en nuestro análisis. Las autoridades sanitarias locales deben buscar ofertas adecuadas de proveedores de servicios en la nube, y obtener las necesarias garantías regulatorias, negociando con cuidado los correspondientes contratos. Asimismo, las autoridades sanitarias locales preocupadas por el cumplimiento de las normativas pueden empezar familiarizándose con las tecnologías en la nube migrando servicios menos críticos, como servicios administrativos (*back-end*), de nóminas, de aprendizaje electrónico o de recursos humanos (aunque siempre hay que tener en cuenta que, muy probablemente, cuando se faciliten servicios de recursos humanos, se procesarán datos confidenciales).

Por otro lado, sería conveniente modificar las normativas para introducir mayor claridad y coherencia en el marco regulatorio de la UE en lo referente a la protección de datos personales, como los datos relativos a pacientes, creando al mismo tiempo condiciones regulatorias viables para los proveedores de servicios en la nube, para así cosechar los beneficios de la informática en la nube aplicada a los servicios de sanidad electrónica. En este sentido:

- Debe realizarse un gran esfuerzo para armonizar la legislación sobre protección de datos en los Estados miembros de la UE.
- Las funciones de protección de datos (del responsable del tratamiento de los datos (*data controller*) y del encargado del tratamiento de los datos (*data processor*)) en el entorno de la nube deben aclararse definitivamente.
- Deben perfeccionarse las iniciativas de autorregulación, como los códigos de conducta o los códigos de prácticas para transferencias internacionales (por ejemplo, normas empresariales vinculantes), a fin de garantizar por completo los derechos de los pacientes en la atención sanitaria transfronteriza internacional.
- Deben proponerse en toda la Unión Europea medidas de seguridad claras y homogéneas, para incorporarlas, en la medida de lo posible, a los servicios en la nube que ofrezcan la llamada "privacidad en el diseño" (*privacy by design*) (19)[51]. Con respecto al concepto de "medidas de seguridad adecuadas", recomendamos el Grupo de Trabajo del Artículo 29.
- Los derechos de los pacientes y los interesados deben armonizarse igualmente en toda la Unión Europea, de forma que los pacientes puedan esperar y disfrutar de una protección uniforme. De esta forma, creemos que un proveedor de servicios en la nube estará en condiciones de preparar ofertas para servicios sanitarios con mayor facilidad, de conformidad con los requisitos jurídicos y regulatorios correspondientes.
- Los proveedores de servicios en la nube deben explicar claramente cómo pueden las autoridades sanitarias locales (y, más en general, sus clientes) migrar a otro proveedor de servicios en la nube (evitando el riesgo de "cautividad del mercado" para las autoridades sanitarias locales) y así garantizar también la continuidad del servicio de las autoridades

[51] *El principio de "Privacidad en el diseño" (Privacy by design)* supone la incorporación de la privacidad y la protección de datos a todo el ciclo de vida de las tecnologías, desde el diseño inicial hasta su aplicación, uso y eliminación final. *Este principio figura entre otros en la comunicación de la Comisión Una Agenda Digital para Europa – COM(2010) 245.*

sanitarias locales durante la transferencia al origen y la migración de información y datos. También se insta a los proveedores de servicios en la nube a ofrecer interoperabilidad.

Servicios informáticos gubernamentales en administraciones públicas municipales: situación núm. 2

Las administraciones públicas utilizan cada vez más la informática para llevar a cabo sus tareas administrativas. Gracias a sus prometedoras ventajas, las administraciones públicas están considerando la posibilidad de migrar sus servicios a infraestructuras informáticas en la nube. El siguiente análisis se centrará en las cuestiones jurídicas relacionadas concretamente con la oferta de servicios basados en la nube, y solo abordará los asuntos relacionados concretamente con nubes de administraciones públicas. ¿Qué normas y normativas deben observarse? ¿Qué deberes y obligaciones deben cumplirse? ¿Cuál es el nivel de riesgo de responsabilidad? Las respuestas a estas preguntas dependen en gran medida de la naturaleza de los servicios que se ofrecen en la nube.

Situación hipotética

El siguiente análisis se centrará en una situación en la que las provincias o regiones configuran y ofrecen una nube como servicio a los municipios (nube privada o comunitaria). A efectos del análisis jurídico, pueden identificarse cuatro partes (sujetos): La región o provincia que es el proveedor de servicios en la nube, el tercero que gestiona la nube, los municipios que la utilizan como abonados y los ciudadanos.

La región o provincia es la propietaria de la infraestructura de la nube, pero su gestión se subcontrata a una entidad privada. Las administraciones públicas serán quienes se encargue de la contratación de este tercero, al que confiarán la configuración y el funcionamiento de la infraestructura de la nube. Los servicios que se van a ofrecer a los municipios se basarán en los modelos PaaS o SaaS. En concreto, estos servicios son los siguientes:

- Gestión electrónica de solicitudes: permitir a los ciudadanos solicitar electrónicamente, desde su hogar, un subsidio, una ayuda, una licencia, noticias sobre la marcha de sus solicitudes, etc.

- Plataforma municipal de gestión / oficina administrativa: contabilidad, recursos humanos, etc. Puede incluir, en concreto, servicios de facturas, bases de datos de ciudadanos (como expedientes penales) y diversos informes automatizados.

- Plataforma de pago en línea: para pagar impuestos, multas, etc.

Tipos de datos y flujo de datos entre las partes implicadas

Dado que se manipulan datos personales, es necesario observar las normas nacionales de cada país sobre la protección de datos.[52] En esta situación, la naturaleza de los datos puede oscilar desde información personal aparentemente poco importante, hasta información altamente confidencial, como expedientes penales y registros relativos a la suspensión del derecho al voto y de licencias.

[52] *Tal y como se establece en la Directiva 95/46/CE sobre protección de datos.*

Deberá tenerse en cuenta la confidencialidad de los datos para los servicios que se ejecutan en la nube, y también para la infraestructura de la nube en sí.
Dada la naturaleza de las llamadas nubes privadas y comunitarias, es decir, infraestructuras que operan bajo el control de la región, de la provincia o de una comunidad de dichas entidades, en circunstancias normales, no habrá flujo de datos no solicitado. Solo podrán trabajar con los datos la región o provincia que gestiona la nube, el municipio y los ciudadanos (por medio de su cliente electrónico).

Cuestiones legales

Legislación aplicable: Directiva sobre Protección de Datos

La Directiva 95/46/CE no diferencia entre el procesamiento de datos por entidades privadas o públicas, es decir, las disposiciones de la Directiva 95/46/CE deberán ser observadas de la misma manera por regiones, provincias y municipios y por entidades privadas. Debe prestarse mucha atención al hecho de que se puedan procesar datos confidenciales en la nube. Esto activa las normas del artículo 8 de la Directiva 95/46/CE, que contiene disposiciones específicas sobre datos confidenciales. Si el servicio en cuestión procesa datos que revelan orígenes étnicos, raciales, opiniones políticas, credos filosóficos o religiosos, pertenencia a sindicatos y datos relativos a la salud o la vida sexual, para gestionarlos deberá cumplir una de las excepciones enumeradas en el artículo 8.2, según su incorporación a la legislación nacional.

Aunque no se puede aplicar a esta situación, debe hacerse notar que, de conformidad con el artículo 13.1, de la Directiva 95/46/CE, los Estados miembros pueden restringir la aplicabilidad de dicha directiva en los casos de seguridad nacional y pública o para el enjuiciamiento y la prevención de delitos. Así, de conformidad con la legislación local en un Estado miembro, puede que algunos tipos de datos gestionados por los municipios no estén sujetos a la Directiva 95/46/CE. En esta situación, no se procesa ese tipo de datos.

La Directiva sobre la Protección de Datos asigna diversos deberes y obligaciones según la función de la entidad en la gestión de datos personales. Este instrumento distingue entre responsable (*controller*) y encargado (*processor*) del tratamiento de los datos (véase el artículo 2.d y e, de la Directiva 95/46/CE).

Dado que son los municipios quienes determinan, como abonados de la nube, los fines y medios concretos del procesamiento de datos, son ellos los responsables del tratamiento de los datos. Como proveedor único de servicios de infraestructuras, que trabaja en representación de su cliente, la región o la provincia es el encargado del tratamiento de los datos. El contratista no gestiona datos. No obstante, deberá ser parte del concepto de seguridad de los datos (ver arriba).

El responsable del tratamiento de los datos es quien debe garantizar el cumplimiento de la legislación sobre protección de datos incorporada a la legislación nacional. Puede que se le pidan responsabilidades si no cumple las normas (artículo 17.2 y 3 de la Directiva 95/46/CE). Para atenuar ese riesgo, el responsable debe solicitar garantías concretas del encargado. Más en concreto, deben aplicarse normas y directrices sobre la gestión de datos. Esto puede llevarse a cabo en forma de

contratos o acuerdos, o de un acto legislativo entre la región o provincia y los municipios, como se solicita en el artículo 17.3 de la Directiva 95/46/CE. Dichos acuerdos deben tener en cuenta la confidencialidad de los datos, según el servicio concreto que se vaya a ofrecer. A continuación, se ofrecerán directrices sobre las condiciones entre estas partes (de conformidad con las recomendaciones jurídicas). Asimismo, debe hacerse notar que tanto el responsable como el encargado deberán garantizar la selección y la supervisión de un tercer contratista fiable que gestione la nube. Esta tarea debe formar parte del concepto de seguridad para el servicio gubernamental de la nube.

De conformidad con el artículo 20 y en consonancia con la legislación nacional, puede que sea necesario llevar a cabo comprobaciones antes del procesamiento, según el tipo de servicio y de los tipos de datos que se van a procesar.

Legislación aplicable: adquisiciones del sector público

Dado que se debe contratar a un tercero para configurar y mantener la infraestructura de la nube, deben observarse las normativas de la UE sobre adquisiciones del sector público.[53] En ese sentido, no habrá una diferencia significativa con respecto a las adquisiciones en otras áreas, por lo que las provincias, las regiones y los municipios deberán aplicar sus conocimientos y experiencias en relación con la legislación y la normativa aplicable.

Legislación aplicable: contratos

En esta situación, el municipio formaliza un contrato con la región o provincia que, a su vez, emplea a un tercero para gestionar la nube. Los requisitos jurídicos relativos a las regiones o provincias deben reflejarse en la cadena contractual. Esto se aplica especialmente a los requisitos sobre el responsable y el encargado de los datos, que ya se han expuesto. A continuación, se incluirán recomendaciones sobre las condiciones contractuales que puedan reflejar y garantizar el cumplimiento de estos requisitos.

Legislación aplicable: leyes de procedimiento civil y penal

Los operadores de servicios en la nube deben ser conscientes del hecho de que, tal vez, se soliciten datos almacenados en la nube como pruebas en procesos civiles o penales. Al existir relaciones entre varias partes en esta situación, son varias las personas que pueden recibir citaciones o solicitudes para transferir pruebas. Esto plantea el problema de a quién dirigir esas solicitudes. De igual forma, deberá tenerse cuidado de preservar el principio de soberanía gubernamental, según el cual las administraciones públicas siguen controlando sus datos y solo deben presentarlos cuando así se lo exija la ley. El hecho de colocar datos bajo el control de entidades privadas puede ser arriesgado; por ley, puede que se obligue a las entidades privadas a presentar pruebas que obren en su poder en determinadas circunstancias (16). Puede ser el caso de una empresa con sede en otro país que gestione la infraestructura de la nube en la que se guardan datos de las administraciones públicas. Por

[53] *http://ec.europa.eu/internal_market/publicprocurement/legislation_en.htm*

medio de sus filiales en otros países, esta entidad estaría expuesta a los tribunales de otros países. Por ejemplo, podrían surgir este tipo de problemas en el proceso de obtención de datos para fines judiciales (*pre-trial discovery*) de las jurisdicciones angloamericanas.[54]

El Grupo de Trabajo del Artículo 29 ha elaborado un documento[55] en el que se abordan las cuestiones prácticas que plantea la gestión de una solicitud de ese tipo.

Consideraciones finales

Uno de los principales problemas legales a los que tienen que hacer frente los gobiernos y las autoridades públicas en general, es la soberanía y el control sobre la información tratada. Los órganos gubernamentales autorizados legalmente para el tratamiento de la información conservan la responsabilidad de tratar esta información de forma adecuada, y deben garantizar que sus obligaciones relativas a la protección de la información se extiendan a los proveedores mediante contrato. En aquellos casos en los que la infraestructura de la nube va más allá de la jurisdicción legal local, el órgano público debe considerar las implicaciones y garantías asociadas ofrecidas por sus proveedores. Si la información de las administraciones públicas es tratada por una entidad privada en una jurisdicción extranjera, existe el riesgo de que los tribunales extranjeros citen a la entidad privada y esto afecte a la información gubernamental. Por lo tanto, los órganos gubernamentales deben garantizar que los proveedores externos imponen medidas adecuadas de seguridad y que existe una serie de mecanismos y procedimientos que garantizan que, en respuesta a una demanda legítima de una autoridad judicial, sólo se entregará la información pertinente.[56]

El cumplimiento de los requisitos legales por todas las partes que participan en una nube gubernamental debe implementarse a través de las relaciones contractuales. En la práctica, o bien se negocian cláusulas que garanticen el cumplimiento de los requisitos legales exigidos o bien se decide formalizar contratos únicamente con aquellos socios cuyos términos y condiciones estándares incluyan las garantías necesarias. Deben negociarse y/o evaluarse atentamente todas las fases de la cadena contractual entre los municipios, provincias o regiones y el proveedor de servicios externos. Este aspecto es especialmente importante cuando sea de aplicación la protección de la información, ya que la legislación de la UE y la legislación nacional de protección de datos requieren una serie de medidas de seguridad en las tecnologías de la información. Se puede trasladar, por ejemplo, en acuerdos de nivel de servicio y provisiones que establezcan las medidas técnicas y organizativas necesarias para garantizar la seguridad en las tecnologías de la información. En la siguiente tabla se muestran las recomendaciones sobre la seguridad de los datos que se derivan, directa o indirectamente, de la Directiva 95/46/CE. Se pueden encontrar recomendaciones y orientaciones complementarias sobre los contratos de servicios de la nube en un estudio anterior de ENISA sobre la computación en la nube[57]

---

[54] *Para más información, véase Geercken/Holden/Rath/Surguy/Stretton, Computer und Recht International 2010, pág. 65.*
[55] *http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp158_en.pdf*
[56] *Esto incluye verificar si las pruebas han sido solicitadas de forma correcta (mediante citación o durante la fase de obtención de datos). Véase el Documento 1/2009 del Grupo de Trabajo del Artículo 29 sobre la presentación de pruebas en la fase previa al juicio en litigios transfronterizos, 11 de febrero de 2009, WP 158; disponible en: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp158_en.pdf*
[57] *http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1662374.*

(15). Debe tenerse en cuenta que la legislación nacional o las políticas gubernamentales pueden requerir garantías específicas adicionales para la información que sea tratada por terceros (privados).

Recomendaciones específicas sobre los servicios en la nube relativas al cumplimiento con la directiva de protección de datos:

Responsabilidad /Obligación	Fuente	Específico para la nube
Capacidad de ser auditados en seguridad de manera espontánea y sin previo aviso	Artículos 16, 17.1	No
Transparencia de información a los interesados en relación con las partes implicadas	Artículos 10 – 12	No
Transparencia de información a los interesados en relación con todos los pasos en el tratamiento de los datos ("flujo de datos")	Artículos 10 – 12	No
Notificación sobre la violación de los datos e incidentes de seguridad	42a BDSG (Alemania)	No
Políticas de seguridad adaptadas a los riesgos	Artículos 17(1)	No

La columna "Específico para la nube" indica si este requisito es específico de la computación en la nube o si es de aplicación general a la contratación externa en TI.

Infraestructura de la nube ofrecida por las administraciones públicas: situación núm. 3

Es posible que las administraciones públicas no solo opten por la computación en la nube como medio para satisfacer sus propias necesidades en el área de la tecnología de la información, sino que también pueden elegir operar una infraestructura de nube como un servicio para sus ciudadanos: el objeto de esta situación. Este último servicio está dirigido fundamentalmente a pequeñas y medianas empresas que puedan alquilar la infraestructura de la nube a las administraciones públicas en un modelo de implementación en la nube. Estas compañías pueden utilizar este servicio para operar y ofrecer Software como Servicio (SaaS). Esto significa que las empresas privadas operarán en "instalaciones" de la nube de las administraciones públicas, lo que implica una serie de problemas legales típicos en este tipo de situación. No obstante, siguen siendo aplicables todos los aspectos tradicionales relativos a la computación en la nube.[58] El siguiente análisis se centrará, por tanto, en los aspectos legales que surgen específicamente cuando se ofrecen servicios basados en la nube, y sólo tratarán algunos de los aspectos más importantes y particulares de las nubes gestionadas por las administraciones públicas.

Tipos de datos y flujo de datos entre sujetos implicados

El modelo de nube de "Infraestructura como Servicio" deja particularmente abiertos los tipos de datos involucrados y la forma de procesar y transmitir los datos. En consecuencia, no es posible predeterminar el tipo de datos personales que se van a gestionar. En este modelo de nube, no existe límite al flujo de datos entre las partes, ni en relación con terceros. El control de los datos corre a cargo de los abonados y sus clientes, y en una nube gubernamental puede haber datos personales y delicados, información confidencial (por ejemplo, *know-how*) y propiedad intelectual.

Cuestiones legales

La presente situación es similar a un entorno de la nube de empresa a empresa (B2B) casi típico. Por tanto, las principales cuestiones relativas a la protección de datos se han señalado ya en el trabajo de ENISA (2009) *Cloud Computing Risk Assessment*[59] y en el apartado pertinente, "Principales cuestiones normativas", en especial las partes relativas a "Confidencialidad y propiedad intelectual", "Responsable del tratamiento de los datos-Encargado del tratamiento de los datos", "Medidas técnicas y organizativas adecuadas de seguridad de los datos", "Transferencia de datos a países fuera del Espacio Económico Europeo", "Derecho de acceso a los datos por parte de los interesados", "Disposiciones sobre Interoperabilidad / Transferencia al origen / Cautividad del mercado", "Negligencia de los proveedores profesionales de servicios en la nube" (aplíquese aquí *mutatis mutandis*).[60]

---

[58] *ENISA (2009) Cloud Computing Risk Assessment, pág. 97 y siguientes. Disponible en:* <*http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport*>.

[59] *Id.*

[60] Si desea consultar un análisis de estas cuestiones en el entorno de la nube de empresa a empresa, consulte el documento de debate del Consejo de Europa (2010) *Cloud computing and its implications on data protection*. Disponible en: <*http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-*

Ley aplicable: Tratado sobre el Funcionamiento de la Unión Europea

Cuando las administraciones públicas de la UE deciden apoyar la computación en la nube, debe considerar las normas establecidas en los Art. 107–109 del TFUE.[61] Estas disposiciones prohíben las ayudas de las administraciones públicas que distorsionen o amenacen con distorsionar la competencia favoreciendo a ciertas empresas. Una infraestructura de una administración pública en la nube puede violar estas normas de tres maneras: En primer lugar, puede distorsionar la competencia favoreciendo la informática en la nube en detrimento de otras formas más tradicionales de subcontratación de TI. En segundo lugar, la competencia se puede ver afectada si solo se alquilan infraestructuras a clientes nacionales y, por último, puede afectar negativamente a otros proveedores privados de la nube.

Ley aplicable: Directiva sobre Comercio Electrónico

Dado que pueden considerarse servicios de la sociedad de la información,[62] las nubes de las administraciones públicas están sujetas a las normas contenidas en la Directiva sobre Comercio Electrónico.[63] En tanto que actúan como proveedores de hosts, el art. 14 de la Directiva sobre Comercio Electrónico les protege de responsabilidades por la información almacenada a solicitud de un cliente del servicio. En esta situación, el cliente es el abonado de la nube que, a su vez, establece ofertas SaaS. El art. 14.1.a de la Directiva establece que las administraciones públicas no serán responsables en la medida en que no tengan conocimiento real de la actividad o información ilegal y, en lo que se refiere a una acción por daños y perjuicios, en la medida en que no tengan conocimiento de hechos o circunstancias por los que la actividad o la información revele su carácter ilícito. El art. 14.1.b exige al proveedor retirar la información o impedir el acceso a esta en cuanto se tenga conocimiento de los puntos mencionados.

Es más, el art. 15 aclara que no existe ninguna obligación general de supervisar los datos que se transmitan o almacenen, sin embargo, el contenido almacenado puede constituir un riesgo de resistencia para las administraciones públicas. El considerando 45 de la directiva 2000/31/CE establece que las limitaciones de la responsabilidad no afectan a la posibilidad de entablar acciones de cesación. A efectos prácticos, esto significa que existe la posibilidad de que se cierre todo el servicio de la nube por una orden judicial.

Ley aplicable: contratos

Las relaciones entre las administraciones públicas y otras partes tienen dos vertientes. Por un lado, está el contrato de abastecimiento con el subcontratista privado que opera y gestiona la nube. Por otro, existe una cadena contractual que va desde las administraciones públicas, pasando por el proveedor de software, hasta los consumidores. Los problemas contractuales entre las

---

Presentations/2079_reps_IF10_yvespoullet1b.pdf>; Balboni, P. (2010) Security and Privacy in Cloud Computing: The European Regulatory Approach, Executive Action Report, No.335, The Conference Board, October 2010. Disponible en: <http://common-assurance.com/wp-content/uploads/P_Balboni_Security-and-Privacy-in-Cloud-Computing.-The-European-Regulatory-Approach.pdf>.

[61] *Tratado sobre el Funcionamiento de la Unión Europea, Número de información 2010/C 83/01, págs. 91*

[62] *Como se define en el artículo 1.2 de la Directiva 98/34/CE, enmendado por la Directiva 98/48/CE.*

[63] *Véase el artículo 2.a de la Directiva 2000/31/CE.*

administraciones públicas y el subcontratista giran en torno a las garantías de cumplimiento de la protección de datos y de abastecimiento de las administraciones públicas (ver arriba). Esta cadena contractual puede, sin embargo, cumplir una función muy concreta: son el único medio por el que las administraciones públicas pueden controlar el cumplimiento de ciertos deberes y responsabilidades en relación con lo que se esté ejecutando en la nube, y de protegerse contra posibles responsabilidades conexas.

Consideraciones finales

Limitaciones sobre el tipo de datos y el flujo de datos

Como propietarias de la nube, las administraciones públicas tienen deberes, responsabilidades y obligaciones impuestas por ley y por contrato. Dentro de la cadena contractual, que va desde las administraciones públicas, pasando por el vendedor SaaS, hasta los clientes, ciertas disposiciones pueden garantizar que las administraciones públicas cumplan todas las leyes pertinentes. En la práctica, esto se puede hacer por medio de condiciones estándar que sean obligatorias y no negociables para todos los socios contractuales.

Tratado sobre el Funcionamiento de la Unión Europea

En términos generales, las reglas recogidas en los artículos 107–109 del TFUE se aplican solo si la ayuda de las administraciones públicas reduce selectivamente las cargas económicas o de otro tipo.[64] En esta situación, ese sería el caso si la nube de las administraciones públicas no operara a precios por debajo del mercado. Si opera a precios de mercado, su influencia sobre el mercado no es diferente a la de una infraestructura de nube privada dentro de la UE. Para excluir una violación del artículo 107 del TFUE, la nube gubernamental no debe tener un precio inferior al del servicio ofrecido por sus competidores comerciales en la UE. Los incentivos no económicos sobre competidores privados, como la adherencia estricta a las reglas y normativas de protección de datos, no se pueden considerar una distorsión amenazante del mercado, ya que se espera el cumplimiento de los requisitos legales por parte de cualquier empresa.

No obstante, los precios inferiores a los de los competidores pueden ser compatibles con el mercado interno, de conformidad con el artículo 107.3.c TFUE. Esta disposición permite las ayudas para facilitar el desarrollo de determinadas actividades o áreas económicas. No obstante, la ayuda no debe afectar negativamente a las condiciones de mercado, hasta el punto de contravenir el interés común. De conformidad con el artículo 108 TFUE, es responsabilidad de la Comisión Europea decidir si las administraciones públicas afectan negativamente al mercado, al facilitar ayuda a los vendedores SaaS en forma de precios no competitivos.

Directiva sobre Comercio Electrónico

[64] *ECJ, orden del 18 de febrero de 1960, De gezamenlijke Steenkolenmijnen in Limburg / ECSC High Authority (30/59, ECR 1961 pág. 48) (FR1961/00091 NL1961/00093 DE1961/00099 IT1961/00089 EN1961/00048 ES1961-1963/00049), disponible en: http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!CELEXnumdoc&lg=en&numdoc=61959O0030*

Legalmente, no existe ninguna obligación de supervisar la información transmitida o almacenada en un entorno de la nube. Sin embargo, el artículo 14 puede ofrecer a los proveedores que actúan como hosts un puerto seguro frente a responsabilidades por contenido ilegal cuando, por ejemplo, eliminen o desactiven el acceso a información al saber o darse cuenta de que el material es ilegal o viola la ley. Las administraciones públicas deben garantizar que exista un procedimiento y un sistema de aviso y eliminación en el caso de que se deba eliminar de la nube material ilegal o que viole la ley. Es preciso que los proveedores de servicios que deseen aprovechar el puerto seguro de la Directiva sobre Comercio Electrónico tomen precauciones, diseñando servicios en la nube de forma que, por ejemplo, se pueda eliminar a unos abonados concretos de la nube para cumplir una orden judicial.

Anexo II – Situaciones hipotéticas

Situación hipotética de atención sanitaria – situación núm. 1

Se trata de Europa, en el año 2011, y las autoridades sanitarias locales deben implementar un nuevo servicio destinado a los ciudadanos: las historias clínicas electrónicas.
Una historia clínica electrónica (HCE) es un registro electrónico de la información sanitaria de un paciente generada por una o más visitas médicas en cualquier ámbito de la atención sanitaria. Esta información incluye datos demográficos del paciente, notas de los progresos, problemas, medicación, signos vitales, antecedentes médicos, vacunas, datos de laboratorio e informes de radiología.

- La HCE representa para los médicos una fuente de información centralizada en el paciente que es segura, en tiempo real y procede del centro de atención.
- La HCE ayuda a los médicos a tomar decisiones mediante el acceso a la información registrada sobre la salud de los pacientes donde y cuando la necesiten y mediante la incorporación de ayuda para la toma de decisiones basada en la evidencia.
- La HCE automatiza y racionaliza el flujo de trabajo clínico, cerrando bucles en la comunicación y la respuesta que puede dar lugar a retrasos o deficiencias en la atención.
- La HCE también puede ser útil para la recopilación de datos para usos distintos a la atención clínica directa, tales como facturación, gestión de la calidad, informes de resultados, planificación de recursos y vigilancia de enfermedades que afecten a la salud pública y sus correspondientes informes.

Con el fin de cumplir con las recomendaciones europeas[65] y los requisitos nacionales y sacar el máximo provecho de los servicios de sanidad electrónica, se debe garantizar la interoperabilidad entre las diferentes historias clínicas electrónicas locales y nacionales. Por ejemplo, la Comisión Europea

[65] *Comisión Europea: e-Health – making healthcare better for European citizens: An action plan for a European e-health Area. Comunicación de la Comisión al Consejo, el Parlamento Europeo, el Comité Económico y Social Europeo y el Comité de las Regiones, COM(2004) 356 final, Bruselas, 30 de abril de 2004. Para más información sobre la estrategia de la Comisión sobre sanidad electrónica, véase ICT for Health y i2010: Transforming the European healthcare landscape: Towards a strategy for ICT for Health, Oficina de Publicaciones de la Unión Europea, Luxemburgo, 2006. El objetivo final es permitir el acceso a la historia clínica electrónica y a los datos de emergencia del paciente desde cualquier lugar de Europa.*

publicó un plan de acción sobre sanidad electrónica en 2004 y, en julio de 2008, una recomendación sobre interoperabilidad transfronteriza de los sistemas HCE (http://www.semantichealth.org/PUBLIC/20080516/P01-03-Semantic%20WS%20Gerard%20Comyn.pdf) para que los médicos pudieran tener acceso a información vital sobre pacientes procedentes de otros Estados Miembros en los que éstos habían sido tratados.

Situación hipotética para la nube

Dado que los modelos de nube se centran mucho en la interoperabilidad y el impacto positivo potencial en la eficiencia de las empresas, una serie de autoridades sanitarias locales (ASL) están considerando la posibilidad de cerrar un acuerdo con una empresa de telecomunicaciones nacional para la creación de su propia nube.

Las ASL planean migrar, a la nube, servicios tales como las historias clínicas electrónicas[66], archivos sanitarios electrónicos (ASE[67]), la programación en línea de las citas para exámenes médicos y otros servicios menos críticos, p.ej., servicios administrativos (*back-end*), recursos humanos, nóminas y aprendizaje electrónico.

Marco Rossi, Director General de una ASL, es uno de los principales patrocinadores del enfoque de la nube, pero es consciente de que los representantes de otras ASL en su región se muestran reacios a trasladar servicios a la nube y, por tanto, él necesita esgrimir argumentos sólidos, en particular en lo que se refiere a disponibilidad de datos y servicios, autenticidad de datos, integridad, resistencia de la seguridad de la información, resistencia de los servicios, protección de los datos personales y cumplimiento de la legislación (en especial respecto a la legislación de protección de datos).

Sabe que en la próxima y decisiva reunión con los directores generales de las demás ASL que puedan estar potencialmente interesados en la "nube híbrida regional de sanidad electrónica", deberá abordar las siguientes preguntas:

- ¿Cuál es el verdadero valor añadido de la nube híbrida regional de sanidad electrónica en términos de resistencia y fiabilidad?
- ¿Puede la oferta de nubes regional ofrecer, por lo menos, el mismo nivel de resistencia y seguridad de datos que el que poseen las ASL actualmente? ¿Pueden fijarse estos requisitos en los acuerdos sobre niveles de infraestructuras de servicio entre las ASL y los proveedores de infraestructura en la nube? ¿Qué servicios o información tendrá potencialmente mayor riesgo y cuál de ellos podría ser incluso más seguro de lo que es en la actualidad?

---

67 "...el archivo sanitario es un archivo creado por un organismo de atención sanitaria que actúa como el responsable único del tratamiento de los datos (p. ej., un hospital o una residencia), en el que trabajan varios profesionales sanitarios. Por el contrario, la historia clínica electrónica es un archivo creado por la agrupación de datos procedentes de responsables del tratamiento de los datos que, por regla general (aunque no es siempre el caso), operan dentro de la misma zona geográfica (p. ej., una unidad de atención médica y un laboratorio privado que operan en la misma región o área). Los archivos sanitarios, por ejemplo, también pueden estar constituidos por el conjunto de informes de salud en poder de los responsables de datos individuales que participan en una iniciativa de HCE a nivel regional."

- ¿Qué tipo de acceso se puede desarrollar de modo que los niveles de seguridad requeridos se puedan aplicar?
- ¿Cómo deben las ASL abordar el cumplimiento de auditoría, jurídico y de las normativas? ¿Qué tipo de procesos de auditoría y flujo de trabajo deben aplicarse?
- ¿Qué modelo de implementación (privado, público, híbrido, comunitario) se adapta mejor a las autoridades sanitarias locales? ¿Deben los servicios públicos (p. ej., almacenamiento de las historias clínicas) residir en el mismo servicio de nube como servicios administrativos y de control (p. ej., nóminas, recursos humanos, etc.)?
- ¿Qué modelo de servicio (IaaS, PaaS o SaaS) se adapta mejor a las necesidades de las ASL? ¿Cuál de estos modelos proporciona la mejor combinación (si existe) entre los modelos de servicios y los servicios (p. ej., la recopilación en línea de archivos sanitarios, programación de citas en línea y otros servicios menos críticos, p.ej., servicios administrativos (*back-end*), recursos humanos, nóminas, aprendizaje electrónico)? Teniendo en cuenta los diferentes requisitos de servicio, ¿qué tipos de acuerdos de nivel de servicio (ANS) se deben aplicar?
- ¿Cómo va a gestionarse el diseño, implementación y administración de la infraestructura a través de las diversas ASL?
- ¿Existen problemas de interoperabilidad entre el sistema de nube y los existentes actualmente que producen los datos médicos en algunos hospitales? ¿Cómo se podrán superar? ¿Cuáles son los requisitos mínimos para la interoperabilidad de las historias clínicas electrónicas?
- ¿Cuál es el verdadero valor añadido de la nube híbrida regional de sanidad electrónica en términos de reducción en el coste de la adquisición y el mantenimiento de TI?
- ¿Cómo puede la ASL garantizar los controles de seguridad efectivos en la solución de extremo a extremo resultante? ¿Qué formas de auditorías, acuerdos de nivel de servicio, sanciones o incentivos económicos, etc., funcionarán mejor para ofrecer una garantía adecuada?
- ¿Qué va a cambiar (si es que cambia algo) en términos de la prestación de los servicios relevantes a los pacientes y de la usabilidad de dichos servicios por parte de los profesionales (p. ej., médicos de hospitales, médicos de medicina general, personal de una ASL)?

Historia clínica electrónica (HCE)

Una *historia clínica electrónica* (HCE) es un almacén de información sobre el estado de salud de un paciente en un formato procesable por el ordenador, guardado y transmitido de forma segura y accesible por múltiples usuarios autorizados. Posee un modelo lógico de información normalizado o decidido de común acuerdo que es independiente de los sistemas de HCE. Su objetivo principal es el apoyo a la atención sanitaria integrada continua, eficiente y de calidad y contiene información que es retrospectiva, concurrente y prospectiva[68].

- La HCE representa para los médicos una fuente de información centralizada en el paciente que es segura, en tiempo real y procede del centro de atención.

[68] *ISO/TR 20514:2005(E)*

- La HCE ayuda a los médicos a tomar decisiones mediante el acceso a la información registrada sobre la salud de los pacientes donde y cuando la necesiten y mediante la incorporación de ayuda para la toma de decisiones basada en la evidencia.
- La HCE automatiza y racionaliza el flujo de trabajo clínico, cerrando bucles en la comunicación y la respuesta que puede dar lugar a retrasos o deficiencias en la atención.

Atributos y requisitos esenciales[69]

El sistema de HCE debe:

- Proporcionar un acceso seguro, fiable y en tiempo real a la información de la historia clínica del paciente donde y cuando se necesite para ayudar en la atención a dicho paciente.
- Garantizar la confidencialidad y seguridad de la información sanitaria del paciente.
- Ser accesible y fiable en todo momento.
- Ser lo suficientemente adaptativa para integrarse con el flujo de trabajo clínico.
- Ser accesible cuando se necesite, en hospitales y ambulatorios, con acceso remoto.
- Capturar y gestionar la información de la historia clínica electrónica episódica y longitudinal.
    - Verificar la información capturada o importada y proporcionar registros de fecha y hora, la fuente de información y modificar el registro de auditoría.
    - Cumplir con las normas industriales aprobadas para el vocabulario y el contenido de mensajes.
    - Aceptar la información procedente de sistemas externos y dispositivos automatizados de captura de datos, tales como monitores de pacientes, equipos de análisis de laboratorio y escáneres de código de barra.
    - En condiciones ideales, aceptar e integrar la información de la historia clínica procedente de fuera de la propia organización, incluida la información de administración de medicamentos de las farmacias de la comunidad.
    - Proporcionar herramientas para una identificación única del paciente y la integración de la información a través de los sistemas y configuraciones sin un identificador común del paciente.
    - Permitir la entrada de datos eficiente de todas las órdenes y documentación por parte médicos autorizados. Esto incluye la gestión de la escritura y reposición de recetas médicas. En condiciones ideales, debería ser compatible con diversos medios de entrada habituales en el sector médico (p. ej., reconocimiento por teclado, voz, puntero o escritura manual). En principio, la documentación debería incluir el razonamiento y base teórica médica.
    - Permitir la firma electrónica, cuando lo permita la ley.
    - Aceptar la información sanitaria del paciente declarada por él mismo.
    - En condiciones ideales, diferenciar entre los datos históricos del paciente (aplicable a través de visitas y en todo el espectro de la atención, p.ej., alergias) frente a los datos episódicos (aplicable a una visita, p.ej., los sonidos respiratorios de la última

[69] *Los atributos de servicio y sus requisitos esenciales se basan principalmente en:* http://www.himss.org/content/files/EHRAttributes.pdf

evaluación respiratoria) y permitir la copia de datos cuando corresponda para apoyar la continuidad de la atención, la precisión de los pedidos y la eficiencia de la documentación médica.

Archivos electrónicos sanitarios

Un *archivo sanitario* presenta los mismos atributos esenciales que las historias clínicas electrónicas, la única diferencia es que el archivo está creado por un organismo de atención sanitaria que actúa como responsable único de los datos (p. ej., un hospital o una residencia) en el que trabajan varios profesionales sanitarios. Por el contrario, la *historia clínica electrónica* es un archivo creado por la agrupación de datos procedentes de diferentes responsables de datos que, por regla general (aunque no es siempre el caso), operan dentro de la misma zona geográfica (p. ej., una unidad de atención médica y un laboratorio privado que operan en la misma región o área). Los archivos sanitarios, por ejemplo, también pueden estar constituidos por el conjunto de informes de salud en poder de los responsables de datos individuales que participan en una iniciativa de HCE a nivel regional. (http://www.garanteprivacy.it/garante/doc.jsp?ID=1672821)

Sistema regional de intermediación e intercambio de registros electrónicos de pacientes

Un *sistema regional de intermediación e intercambio de historiales electrónicos de pacientes* es un punto de referencia regional para toda la información sanitaria relacionada con un paciente que vive en esa región.

La información (historiales electrónicos de pacientes) se deposita directamente en un almacén regional compartido con todas las partes interesadas nacionales e internacionales (hospitales y clínicas, médicos de medicina general, etc.) o bien se guarda a nivel local (autoridades sanitarias locales, hospitales, etc.) y se referencia mediante un enlace en el sistema regional de intermediación e intercambio de historiales electrónicos de pacientes.

Son aplicables a este servicio los mismos atributos y requisitos esenciales identificados para la historia clínica electrónica.

Nube comunitaria local y regional – situación núm. 2

Caso práctico de uso de nube en el que participan autoridades locales en España

El gobierno provincial de Jaén, en el sur de España, quiere mejorar la participación de los ciudadanos en la Sociedad de la Información y promover los servicios de la administración electrónica. Para ello ha impulsado un proyecto denominado Jaén Provincia Digital, que tiene cuatro objetivos estratégicos:

1. Proporcionar una infraestructura de comunicaciones digitales en toda la provincia.

2. Mejorar el acceso y la participación de los ciudadanos en la sociedad de la información y del conocimiento.

3. Ofrecer los servicios y recursos de los ayuntamientos en línea.

4. Ofrecer los servicios y recursos del gobierno provincial en línea.

El gobierno provincial ha reconocido el valor de establecer soluciones organizativas y tecnológicas comunes para las administraciones locales.

Esto es lo que el gobierno provincial ha hecho hasta ahora para alcanzar sus cuatro objetivos.

Infraestructura digital

La infraestructura digital se basa en la red provincial de comunicaciones conocida con el nombre de Heraclea, que proporciona acceso de banda ancha a todos los municipios. La red cuenta con un total de 113 conexiones, 77 de las cuales son ayuntamientos y las 36 restantes, oficinas del gobierno municipal. Hasta ahora, el gobierno provincial ha conectado 97 municipios al gobierno provincial a través de GIGADSL, que proporciona los accesos a los servicios municipales en línea.

También facilita el acceso a depósitos de software libre a través de dos redes administrativas: la red del gobierno regional de Andalucía, llamada NEREA, y la red del gobierno estatal, denominada SARA. El gobierno autonómico de Andalucía, del que Jaén es una provincia, ha desarrollado su propia red de distribución Linux, llamada Guadalinex (http://www.guadalinex.org/). Guadalinex posee sus propias herramientas de oficina y ofrece a los ciudadanos acceso libre al software y herramientas de su sistema operativo.

Ciudadanía digital

El programa Ciudadanía digital promueve la igualdad de participación de los ciudadanos de la provincia de Jaén en la sociedad de la información y del conocimiento. En 2001, el gobierno provincial fue uno de los pioneros en la introducción de centros con acceso público a Internet. Treinta y cuatro de los 97 municipios de la provincia estaban equipados con telecentros. Actualmente, todos los municipios cuentan con telecentros. En estos momentos, Jaén dispone de 161 telecentros, de los cuales 62 están situados en pueblos. Los telecentros ofrecen a los ciudadanos acceso gratuito a Internet y, en particular, programas y actividades centradas en el aprendizaje y comercio en línea, así como otros servicios electrónicos.

Ayuntamientos digitales

Jaén y otros gobiernos provinciales de Andalucía se han unido para desarrollar una plataforma común llamada Modelo TIC de Ayuntamiento Digital, que permite la administración y la progresiva implementación de la ciudadanía digital. El modelo tiene tres capas: (1) un portal de servicios en línea; (2) una página web municipal; y (3) un servicio administrativo del ayuntamiento, que se encarga de administrar el censo, la gestión del suelo, el registro, agua, impuestos, contabilidad y nóminas. En abril de 2010, 23 municipios habían usado la plataforma para establecer sus propios portales de servicios en línea. Se espera que todos los municipios sigan su ejemplo.

Gobierno provincial digital

El gobierno provincial ha hecho realidad la administración electrónica al poner todos sus servicios en línea. La versión en papel del *Boletín Provincial* desapareció en diciembre de 2003; el gobierno provincial solo publica actualmente una versión electrónica. Se ha promocionado el software de acceso libre y abierto no solo en su propia página web sino también en las de los municipios.

El gobierno provincial ha puesto en línea su plan estratégico, junto con los indicadores para medir el éxito de su implementación (conocido como cuadro de mando integral). Ha elaborado una *Guía de los Servicios del Gobierno Provincial*, que también se puede consultar en línea. Con el fin de lograr una administración sin papeles, el gobierno provincial ha puesto su registro y comunicaciones electrónicas en línea, así como sus planes de gestión del gasto, subsidios y la gestión tributaria.

Información general

Jaén Provincia Digital es un proyecto para potenciar la cooperación tecnológica y la participación en la sociedad de la información. Este proyecto vincula el gobierno municipal y los 97 ayuntamientos de la provincia. Se basa en los siguientes principios:

- La interoperabilidad y el software libre como base para los componentes del modelo.
- El trabajo en línea compartiendo las redes de comunicación (tanto dentro de la provincia como a nivel andaluz y nacional).
- La definición de modelos comunes de sistemas de gestión e información para la mejora de las administraciones públicas en línea. El modelo de TIC del Ayuntamiento Digital es parte del depósito local de software de Andalucía. No solo se va a aplicar a los municipios de Jaén, sino que también está recomendado y disponible para otros municipios andaluces y del resto de España.

El proyecto está basado en una iniciativa del Ministerio de Industria, Turismo y Comercio español (MITYC), que proporciona la infraestructura, la plataforma y un conjunto de aplicaciones para todos los ayuntamientos españoles (que son 8.300). Las administraciones públicas todavía tienen que moverse a la nube, sin embargo, ya que cada ayuntamiento tiene que descargar, instalar y configurar cada aplicación y, por lo tanto, necesita tener su propia infraestructura.

Entre los servicios prestados por el Ministerio de Industria a los ayuntamientos locales destacan los siguientes:

1 LocalWeb, una aplicación para generar sitios web.

2 SIGEM, una aplicación para gestionar los procedimientos administrativos de un archivo o registro.

3 LocalGIS, una aplicación de gestión de la cartografía.

4 Registro, una aplicación para el mantenimiento del censo de población municipal.

5 Catastro, una aplicación para el registro de las propiedades de ciudadanos y empresas.

6 E-Easy, una aplicación de apoyo a la creación de empresas y la facturación de las entidades locales.

Requisitos de TIC del modelo de Jaén (ficticio, a dos años en el futuro)

El gobierno provincial de Jaén inició su plan Jaén Provincia Digital tras celebrar consultas con sus 97 municipios. En conjunto, identificaron sus requisitos de servicios y recursos, incluyendo una red de distribución, varios servidores, un almacenamiento suficiente y un sistema que permitiera múltiples y variados tipos de aplicaciones y servicios. En concreto, las necesidades previstas eran las siguientes:

- Un *autoservicio a demanda* con el cual cualquier municipio podría disponer de servidor a cualquier hora y de almacenamiento en red cuando lo necesitara, de forma automática, y sin necesidad de interacción humana con el proveedor de cada servicio.
- *Acceso a la red a través de diferentes dispositivos*, como estaciones de trabajo, telecentros, teléfonos móviles, portátiles y PDA.
- *Puesta en común de recursos informáticos* para servir a muchos usuarios diferentes, algunos funcionarios del gobierno municipal y provincial y algunos ciudadanos.
- *Rápida elasticidad*, es decir, la red pudiese responder con rapidez y de forma automática a los cambios en la demanda por parte de municipios concretos o del gobierno provincial.
- *Medición del uso del recurso*, por lo que el sistema podría medir e informar de los diferentes niveles de uso (p. ej., almacenamiento, procesamiento, ancho de banda y cuentas de usuario activas) por parte de los municipios, el gobierno provincial e incluso, los ciudadanos.
- *Migración de los servicios existentes*, de modo que se pudieran seguir usando algunos de los servicios personalizados o especializados en el nuevo sistema.
- *Relación coste-beneficio positiva*, en la que todos los interesados pudieran beneficiarse de costes más bajos que los recursos informáticos diversos que hay estado utilizando en entornos esencialmente autónomos. Además, querían pagar solo por el uso real, y no por recursos que quizás no llegaría a usar.
- *Implementación rápida*: querían poder ofrecer rápidamente nuevos servicios sin tener que adquirir, certificar y validar nuevo hardware y software.
- *Alta disponibilidad y fiabilidad*: querían un sistema con una disponibilidad y resistencia del 100% o, por lo menos, que se aproximara al 100% lo más posible. Si se producía un fallo en un servidor central, querían que cualquier otro servidor se hiciera cargo del servicio de inmediato. Si se producía un fallo en la red (p. ej., debido a un fallo en el suministro energético o por una interrupción en la línea de comunicaciones), deseaban una copia de seguridad instantánea.
- *Facilidad de uso*: querían un sistema con una curva de aprendizaje corta para aquellos que desarrollaban y utilizaban los servicios de las administraciones públicas electrónicas.

Basándose en sus necesidades, se llegó al acuerdo de que debían moverse a la nube, pero de una manera que les permitiera llevarse algunos sistemas de los ya existentes. Hubo cierto debate en torno a qué modelo de servicio sería el más apropiado.

Modelos de servicio

Software como servicio (Software as a Service, SaaS) : muchos ciudadanos-consumidores necesitan utilizar aplicaciones populares (correo electrónico, procesador de textos, hojas de cálculo), así como aplicaciones especializadas (para obtener permisos de aparcamiento, servicios públicos, certificados emitidos por el ayuntamiento, acceso a bibliotecas, etc.) y aplicaciones administrativas (nóminas e impuestos) que podrían estar basadas en la nube y accederse a ellas mediante un navegador web utilizando diferentes dispositivos de usuario (estaciones de trabajo, portátiles, teléfonos móviles y PDA). El ciudadano-consumidor (y el trabajador administrador) solo necesitaría su dispositivo. La nube le proporcionaría el software, las aplicaciones, el almacenamiento y la copia de seguridad.

Plataforma como Servicio (Platform as a Service, PaaS): el gobierno provincial y los municipios utilizan aplicaciones comerciales populares, pero también necesitan desarrollar sus propias aplicaciones especializadas utilizando lenguajes y herramientas de programación admitidos por el proveedor de la nube. El proveedor de la nube gestionaría la red, los servidores, los sistemas operativos y el almacenamiento.

Infraestructura como Servicio (Infrastructure as a Service, IaaS): el gobierno y los municipios valoraron si necesitaban controlar la infraestructura actual (servidores, sistemas operativos, almacenamiento, aplicaciones, etc.) pero decidieron que no era necesario y que sería más económico dejar que un proveedor de nube se encargara de estos temas.

Después de considerar los modelos de implementación (una nube privada, comunitaria, pública o híbrida) decidieron que les convenía una nube comunitaria.

Resistencia

Si bien los beneficios económicos y de otros tipos que representaba moverse a la nube eran evidentes, aún les preocupaba la resistencia del servicio, la seguridad de la información y el cumplimiento legal. El registro del proveedor de la nube, en ese sentido, era mejor que los suyos propios. Aún así, sus preocupaciones en cuanto a resistencia eran las siguientes:

- *Protección de datos* (integridad, privacidad y autenticidad): algunos de sus servicios utilizaban datos personales, por lo que ellos necesitaban garantías de que el proveedor de la nube cumpliría las leyes españolas de protección de datos.
- *Disponibilidad, fiabilidad y calidad de servicio*: necesitaban servicios que estuvieran siempre disponibles y que fueran fiables (es decir, que siempre hicieran aquello que se esperaba).
- *Copias de seguridad y continuidad*: si se produjera una caída del servidor principal de alojamiento, otro debería ser capaz de asumir el control "inmediatamente". Debían tenerse en cuenta varios factores externos, como interrupciones del suministro eléctrico y ataques físicos y cibernéticos.
- *Control del acceso*: algunos servicios podrían ser accesibles para cualquiera, otros (p. ej., servicios sociales) estarían controlados y limitados por individuos seleccionados. El control del acceso debía incluir medidas para la autenticación de los usuarios y proporcionar

registro de auditorías y su seguimiento. En España, es posible acceder a muchos servicios electrónicos de la administración pública utilizando el DNI electrónico, lo cual contribuye a apoyar el modelo de Identidad como Servicio (IDaaS).

- *Auditorías* y certificación: quizás el requisito más difícil establecido por los municipios era que el servicio proporcionado por la nube debía estar sujeto a una auditoría y, en algunos casos o servicios, debía estar certificado de acuerdo con las normas de seguridad (ISMS, ISO 27001).

Procedimientos administrativos electrónicos

Se desarrolló una aplicación para gestionar los procedimientos administrativos de un archivo o registro. Dicha aplicación permite a los ciudadanos solicitar electrónicamente (desde sus casas) subvenciones, ayudas y licencias, o realizar pagos, recibir noticias sobre el estado de sus solicitudes, así como información sobre si falta cualquier documento, con instrucciones sobre cómo adjuntarlos, y finalmente permite recibir una notificación de los resultados de sus gestiones.

Nube gubernamental como vivero de empresas - situación hipotética núm. 3

El Ministro de Comunicaciones y Tecnología y el Ministro de Industria y Desarrollo estaban manteniendo una conversación informal tras una reunión con el Primer Ministro.

El tema sobre el que discutían era el mismo que a menudo habían tratado el año pasado, la computación en la nube.

El Ministro de Industria y Desarrollo le dijo a su colega: —Mantuve una reunión la semana pasada con mi homólogo japonés y me estuvo explicando su proyecto J-SaaS.

El Ministerio de Economía, Comercio e Industria japonés desarrolló una infraestructura de computación hace un año. El sistema se llama J-SaaS. El J-SaaS es una plataforma informática que funciona como vivero para proveedores y usuarios de SaaS.

Los proveedores independientes de software (ISV) centrados en las pymes pueden combinarlo con sus paquetes de aplicaciones y ofrecerlo como SaaS. Los usuarios de las pymes pueden utilizar el servicio tanto para la producción como para uso experimental a un bajo coste. Antes, los ISV japoneses vendían paquetes de software a pymes que tienen poca competencia en TI y escasa deducción por gastos de capital. Si los productos de software de los ISV pueden ofrecerse como SaaS, disminuirán las barreras del mercado. Sin embargo, los ISV no podrían ofrecer SaaS, puesto que no cuentan con la infraestructura para ofrecer SaaS. Así, el gobierno preparó la infraestructura para que los proveedores y usuarios pudieran utilizarla y promover la gestión basada en TI, por el lado del usuario, y el negocio en un nuevo modelo de implementación, por el lado del proveedor.

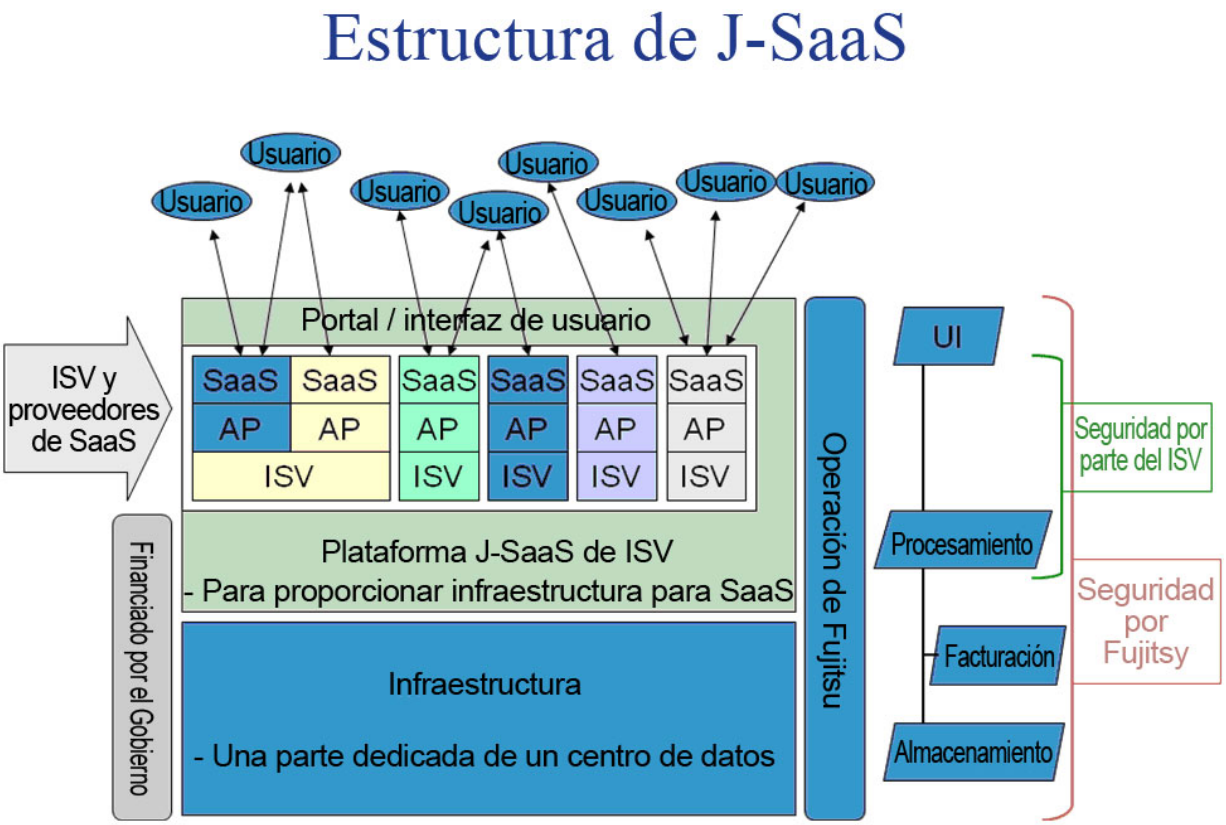
—No había oído hablar de esto —respondió el Ministro de Comunicaciones y Tecnología —. Parece una muy buena idea, que podríamos adoptar en nuestro país y en toda la UE (?) y, sobre todo, si tenemos en cuenta que el 99% de los negocios de la UE son pequeñas y medianas empresas y microempresas. También deberíamos plantearnos la ampliación de los servicios ofrecidos por la nube gubernamental para incluir también IaaS y PaaS.

—Sí, estoy de acuerdo —dijo el Ministro de Industria y Desarrollo—, pero antes de presentar esta idea al público deberíamos tener respuestas concretas y sólidas a las preguntas más habituales sobre computación en la nube:

1. ¿Es lo suficientemente segura?
2. ¿Los ISV son de suficiente confianza (gestión de la confianza entre consumidores e ISV)?
3. ¿Dónde se van a almacenar los datos?
4. ¿La nube gubernamental será lo suficientemente fiable? La nube gubernamental, ¿puede ofrecer un mejor acuerdo de nivel de servicio (ANS) que el ofrecido actualmente a las pymes?
5. ¿La concentración de recursos va a aumentar los incentivos para los atacantes?

6. ¿Es nuestro actual marco jurídico adecuado para enfrentarnos a los posibles desafíos de la nube?
7. ¿Qué modelo de implementación (privado, público, híbrido o comunitario) se adapta mejor a los objetivos?
8. ¿Va a ser de verdad rentable para las pymes?
9. ¿Puede la nube gubernamental adoptar un modelo de ayudas y subvenciones para las pymes con el objetivo de promover el proceso de migración?
10. ¿Va a distorsionar el mercado?
11. ¿Qué ocurre con las infraestructuras críticas?
12. Responsabilidad: ¿pueden las administraciones públicas ofrecerla?
13. ¿Deberá ser supranacional para ser fiable?
14. ¿Podemos definir claramente nuestras expectativas con respecto al riesgo?

Modelo J-SaaS



Teniendo como referencia la estructura del J-SaaS japonés, parece claro que las administraciones públicas pueden ofrecer varios servicios. La visión estratégica del gobierno permitirá decisiones comerciales, en las que se tendrán en cuenta, entre otros factores, las siguientes variables posibles:

Tipo de cliente potencial

- Microempresa.
- Pequeñas y medianas empresas (pymes).
- Empresas que ejercen su actividad comercial en sectores comerciales muy regulados.
- Grandes empresas (que mueven servicios concretos).
- Las categorías mencionadas deben considerarse como usuarios finales de la plataforma y como empresas que aprovechan la nube gubernamental para ofrecer sus servicios de TI a otras empresas.

Necesidades de posibles clientes y administraciones públicas

- Apoyo de negocios nacionales.
- Integración con conjuntos de datos y servicios competentes de las administraciones públicas.
- Infraestructura de TI fiable y rentable a demanda que tenga el potencial de poder llegar a cubrir todo el espectro de servicios de TI.
- Plataforma de TI fiable y rentable a demanda que pueda integrarse o sea compatible con la plataforma de servicios internos.
- Un banco de pruebas con pocos requisitos de disponibilidad.
- Servicios específicos del sector.
- Servicios de seguridad de valor añadido.
- Marca de confianza.
- Cumplimiento legal.
- Asignación clara de responsabilidades.

Anexo III - Descripción de la arquitectura del Proyecto Reservoir

Arquitectura de nube virtual para nubes comunitarias

En este apartado describimos una arquitectura de nube virtual abstracta que ofrece Infraestructura como Servicio (IaaS), Plataforma como Servicio (PaaS) y Software como Servicio (SaaS). La arquitectura presenta una capa de infraestructura virtual encima de la infraestructura física. Esta capa de abstracción está diseñada para gestionar una federación de infraestructuras físicas heterogéneas. Cada sitio tiene una partición de una capa de virtualización en máquinas virtuales (MV) que son módulos de tiempo de ejecución totalmente aislados que abstraen las características físicas del recurso y permiten compartir recursos. Esta arquitectura se basa en tres capas distintas:

- Gestor de servicios / plataformas (GS): es responsable de instanciar la aplicación de servicio solicitando la creación y configuración de una MV para cada componente de servicio, de acuerdo con la definición de servicio, garantizando así el cumplimiento del acuerdo de nivel de servicio (ANS). En el caso de una plataforma, distribuye el código en la plataforma apropiada, p. ej. en un contenedor de servicios java.

- Gestión de infraestructuras virtuales (GIV): es responsable de situar las MV en máquinas host (MH). Recibe solicitudes del GS para crear y redimensionar MV y decide la mejor ubicación para que estas MV optimicen una función de utilidad de sitio dado un conjunto de limitaciones (que establece el GS). El GIV no solo gestiona la provisión de las MV, sino también de las redes virtuales (RV) y el almacenamiento virtual (AV) necesario. El GIV controla totalmente las MH. Un motor de políticas (MP) es un componente de GIV responsable de ubicar y migrar las MV en una MH. La MV representa un recurso virtualizado que aloja cierto tipo de MV. Los GIV emiten comandos genéricos para gestionar el ciclo de vida de las MV, y estas son responsables de traducir estos comandos a comandos específicos para la plataforma de virtualización que abstrae cada MV.

- Gestor de infraestructuras físicas (GIF): Esta capa gestiona la máquina física, la conexión a red y el equipo de almacenamiento. Gestiona la adición y eliminación de recursos del conjunto de recursos compartibles.

Como se muestra en la figura, cada capa tiene un componente de gestión para gestionar los servicios y plataformas, la infraestructura virtual y la infraestructura física.

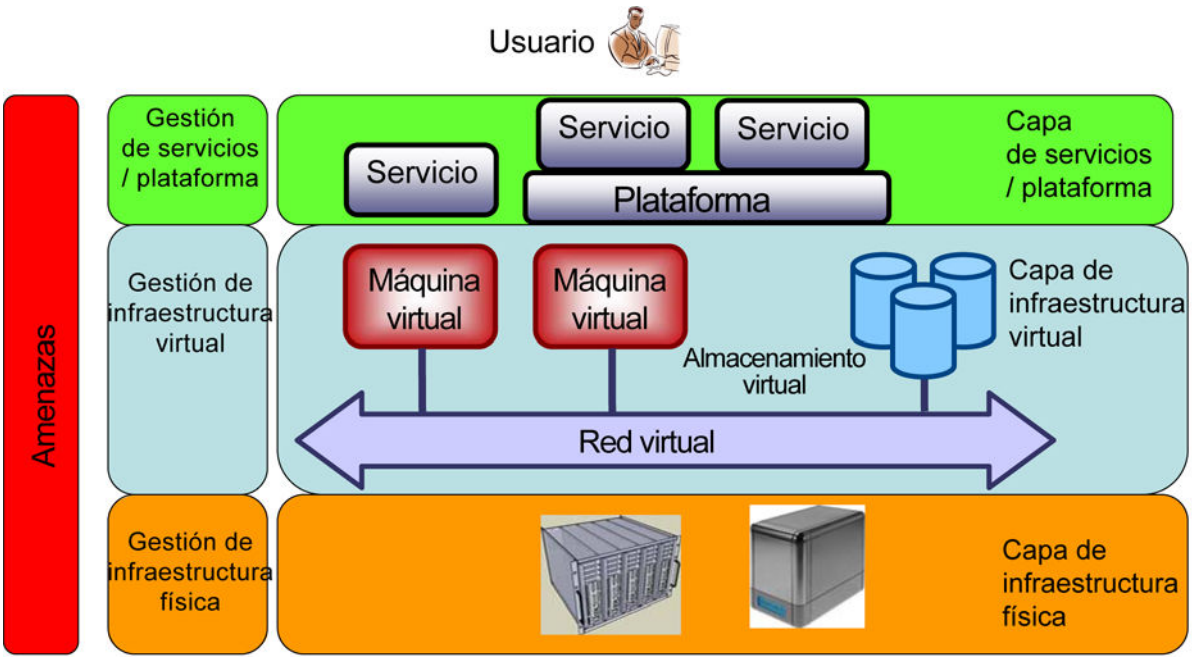


FIGURA 2 AMENAZAS DE EXTREMO A EXTREMO A LA RESISTENCIA

Amenazas de extremo a extremo a la resistencia de una arquitectura de nube virtualizada

Varios tipos de usuarios acceden a la nube mediante la conexión de red: el proveedor de servicios que distribuye y gestiona su aplicación de varios niveles en la nube, el administrador de la infraestructura virtual que gestiona esta y el usuario final que accede a las aplicaciones que se ejecutan en la infraestructura de nube. Estos distintos tipos de usuarios de nube son fuentes de amenazas. Deben identificarse y deben establecerse contramedidas.
La resistencia de la nube de extremo a extremo puede verse amenazada en cualquier capa de una arquitectura de nube virtualizada. En la tabla inferior se clasifican ciertas amenazas importantes para cada capa descrita en la Figura 2 y los componentes que se ven amenazados:

Amenaza	Capa	Componente amenazado
Error de servicio de facturación o disponibilidad reducida	Servicio o plataforma	GS
Menor disponibilidad o error al crear la MV	Infraestructura virtual	GIV, MV, RV, AV
Menor disponibilidad o error al cerrar la MV	Infraestructura virtual	GIV
Menor disponibilidad o error de la función de migración	Infraestructura virtual	GIV
Menor disponibilidad de la función de control	Servicio o plataforma, infraestructura virtual	

Amenaza	Capa	Componente amenazado
Interrupciones de la red	Infraestructura física	Red
Compromiso de la gestión de red	Infraestructura física	Red
Interferencia de aplicaciones	Servicio o plataforma, infraestructura virtual	GS, GIV, MV, RV, AV
Sobrecarga del sistema, incapacidad de escalar	Infraestructura virtual	GIV
Compromiso del hipervisor o el SO	Infraestructura virtual	MV
Compromiso de la interfaz de gestión	Infraestructura virtual o física	GIV, GIF
Compromiso del sistema o proveedor de la gestión de identidades	Servicio o plataforma, infraestructura virtual o física	Servicio, GIV, GIF
Ataque DDoS o DOS a otra autoridad sanitaria que afecta a sus sistemas	Servicio o plataforma, infraestructura virtual o física	GS, GIV, GIF, servicio, plataforma
Compromiso o fallo del sistema de contabilidad y facturación	Servicio o plataforma	GS
No disponibilidad del servicio HCE o de otro servicio	Servicio	Servicio
Pérdida o compromiso de la información de HCE	Servicio	Servicio
Incoherencia de datos	Servicio	Servicio
Desastres	Todos	Todos
Claves de cifrado perdidas	Todos	Todos
Bancarrota del socio o proveedor de la nube	Todos	Todos

Amenazas a la resistencia de extremo a extremo en nubes comunitarias

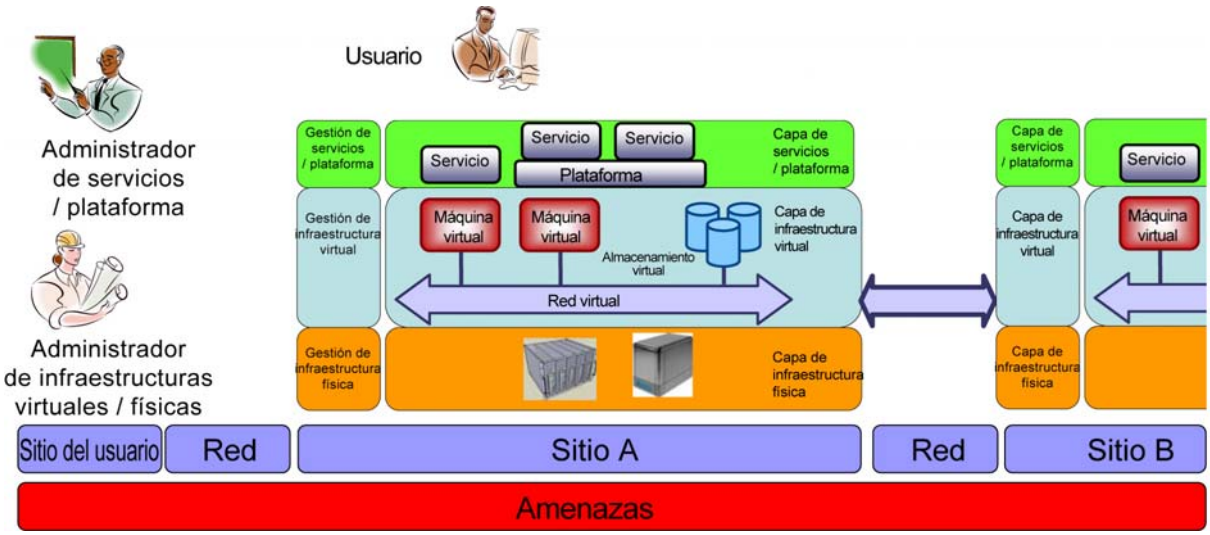


FIGURA 3 AMENAZAS DE EXTREMO A EXTREMO A LA RESISTENCIA EN NUBES COMUNITARIAS

En el caso de nubes comunitarias basadas en una federación de centros de datos, estos centros están conectados por redes físicas y también virtuales. Por lo tanto, la resistencia de extremo a extremo afronta distintas amenazas que en el caso de una sola nube. Además de las amenazas a las distintas capas presentadas en el apartado anterior, deben tenerse en cuenta otras amenazas a la estructura de la federación de nube subyacente.

La Figura 3 muestra una nube comunitaria compuesta pore dos sitios, A y B. Los dos sitios están conectados mediante redes y redes virtuales. Los dos sitios pueden ofrecer recursos desde cada uno de los sitios. La figura muestra los tres tipos de usuarios de nubes (usuario final, administrador de servicios o plataformas y administrador de infraestructuras virtuales o físicas). Las amenazas pueden ocurrir en cualquier lugar: en el sitio del usuario de la nube, en la red entre el sitio del usuario de la nube y en el sitio de la nube principal, en la red entre los dos sitios de nube y en el segundo sitio de nube.

La tabla inferior clasifica las amenazas principales según la ubicación de la amenaza en la Figura 3 y los componentes amenazados:

Amenaza	Ubicación	Componentes amenazados
Error de servicio de facturación o disponibilidad reducida	Sitio de la nube	GS
Menor disponibilidad o error al crear la MV	Sitio de la nube	GIV, MV, RV, AV

Amenaza	Ubicación	Componentes amenazados
Menor disponibilidad o error al cerrar la MV	Sitio de la nube	GIV
Menor disponibilidad o error de la función de migración	Sitio de la nube	GIV
Menor disponibilidad de la función de control	Sitio de la nube	
Interrupciones de la red	Usuario de red de nube, red comunitaria	Red
Compromiso de la gestión de la red	Usuario de red de nube, red comunitaria	Red
Interferencia de aplicaciones	Sitio de la nube	GS, GIV, MV, RV, AV
Sobrecarga del sistema, incapacidad de escalar	Sitio de la nube	GIV
Compromiso del hipervisor o el SO	Sitio de la nube	MV
Compromiso de la interfaz de gestión	Sitio de la nube	GIV, GIF
Compromiso del sistema o el proveedor de la gestión de identidades	Sitio de la nube	Servicio, GIV, GIF
Ataque DDoS o DOS a otra autoridad sanitaria que afecta a sus sistemas	Sitio de la nube	GS, GIV, GIF, servicio, plataforma
Modificación del tráfico de red	Usuario de red de nube, red comunitaria	Red, red virtual
Compromiso o fallo del sistema de contabilidad y facturación	Sitio de la nube	GS
No disponibilidad del servicio HCE o de otro servicio	Sitio de la nube	Servicio
Pérdida o compromiso de información de HCE	Sitio de la nube	Servicio
Incoherencia de datos	Sitio de la nube	Servicio
Claves de cifrado perdidas	Sitio de la nube	Todos

Anexo IV – Lista de amenazas

ID	Descripción de amenaza
Amenazas aplicables a todas las situaciones	
1.	Interrupciones de red (pérdida temporal de componentes de enrutamiento, asumiendo que puede recuperarse)
2.	Pérdida de tráfico
3.	Gestión de red (es decir, congestión de red, mala conexión, uso no óptimo, etc.)
4.	Interferencia de aplicaciones (acceso al código, y posterior ataque)
5.	Error del administrador del PN
6.	Intruso malicioso (exploración ineficaz, registros ineficaces, etc.)
7.	Recursos agotados del PN (pérdida de rendimiento)
8.	Sobrecarga del sistema, incapacidad de escalar
9.	Compromisos del hipervisor o del SO
10.	Ataques de ingeniería social (suplantación – ej. seguridad a demanda)
11.	Filtración de datos en la carga o descarga dentro de la nube (*sniffing* (captura de paquetes), *spoofing* (suplantación de identidad), ataques por canal lateral, etc.)
12.	Compromiso de la interfaz de gestión (manipulación, disponibilidad de infraestructura)
13.	Proveedor o sistema de gestión de identidades (es el punto de error del sistema)
14.	DDoS
15.	DOS en otra autoridad sanitaria que afecta a la suya
16.	Emprender exploraciones o sondeos maliciosos
17.	Modificación del tráfico de red
18.	Escalada de privilegios
19.	Robo de equipo informático
20.	Compromiso o fallo del sistema de contabilidad y facturación
21.	Repetición
22.	Abordaje al sistema anfitrión (hacer compartimentos)
23.	Indisponibilidad del servicio de HCE
24.	Otra indisponibilidad de servicio
25.	Pérdida o compromiso de información de HCE
26.	Duplicación de datos
27.	Incoherencia de datos (actualización de datos inefectiva)
28.	Pérdida o compromiso de registros operativos
29.	Pérdida o compromiso de registros de seguridad (manipulación de investigación forense)
30.	Interceptación de datos durante la migración o actualización periódica de datos en la nube

ID	Descripción de amenaza
31.	Compromiso de los datos durante la migración o actualización periódica de datos en la nube
32.	Desastres (naturales)
33.	Acceso no autorizado a los locales (incluido el acceso físico a máquinas y otras instalaciones)
34.	Robo de copias de seguridad
35.	Claves de cifrado perdidas
36.	Eliminación insegura de datos (cuando lo solicita el paciente)
37.	Pérdida de gobernanza, control, especificaciones (el ANS puede estar incompleto; no cubre todos los indicadores principales de rendimiento)
38.	Bancarrota del socio o proveedor de la nube
39.	Adquisición del proveedor o socio de la nube (aumenta la probabilidad del cambio estratégico y puede poner en riesgo acuerdos no vinculantes)
40.	Responsabilidad respecto a normativas (por ejemplo, notificación a los clientes de incumplimientos sobre la seguridad de los datos)
41.	Problemas de protección de datos y legales
42.	Conflicto de requisitos de privacidad y seguridad
43.	Conflictos entre directrices locales o regionales (necesidad de aplicación)
Amenazas específicas al modelo de nube comunitaria y, más en concreto, al enfoque federado propuesto en el proyecto RESERVOIR.	
44.	Error de servicio de facturación o disponibilidad reducida: el usuario de IaaS solicita su factura según el pago por uso. Cualquier reducción en la disponibilidad del servicio de facturación afectará a la resistencia de IaaS.
45.	Menor disponibilidad o fallo al crear EEV (entornos de ejecución virtuales): la configuración de EEV conlleva descargar las imágenes del sistema, instanciando después con los parámetros de configuración, iniciándolas y creando la red virtual entre el EEV. Cualquier reducción de disponibilidad al iniciar el EEV afectará a la resistencia de IaaS.
46.	Menor disponibilidad o error al cerrar el EEV: elimina un EEV tras una solicitud sin distribuir. Cualquier reducción de disponibilidad al cerrar el EEV afectará a la resistencia de IaaS.
47.	Menor disponibilidad o error de la función de migración: la migración permite volver a buscar un EEV de un host a otro sin interrumpir el servicio. Cualquier fallo en la función de migración afectará en general a la resistencia de IaaS.
48.	Menor disponibilidad de la función de control: el control de EEV permite evaluar la infraestructura y tomar acciones correctivas si es necesario, como restablecer, escalar o migrar EEV. Cualquier reducción de disponibilidad en el control de la infraestructura afectará en general a la resistencia de IaaS.
49.	Error de servicio de facturación o disponibilidad reducida: el usuario de IaaS solicita su factura según el pago por uso. Cualquier reducción en la disponibilidad del servicio de facturación afectará a la resistencia de IaaS.