


**GUÍAS DE SEGURIDAD
DE ÁREAS CRÍTICAS EN
CLOUD COMPUTING
V3.0**

INTRODUCCIÓN

INTRODUCCIÓN

Este documento constituye la tercera versión de la "Guía de Seguridad para las áreas críticas de atención en Cloud Computing" de la Cloud Security Alliance, que fue publicada originalmente en abril de 2009.

Las distintas versiones de la Guía, en su idioma original, se encuentran disponibles en las siguientes ubicaciones:

<http://www.cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf> (Versión 3 de las guías en inglés)

<http://www.cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf> (Versión 2 de las guías en inglés)

<http://www.cloudsecurityalliance.org/guidance/csaguide.v1.0.pdf> (Versión 1 de las guías en inglés)

Por su parte, las traducciones al Castellano, llevadas a cabo por la Asociación Española para el Fomento de la Seguridad de la Información (ISMS Forum) y el Capítulo español de la Cloud Security Alliance (CSA-ES), se encuentran disponibles en:

<https://www.ismsforum.es/noticias/389/el-capitulo-espanol-de-csa-publica-la-traduccion-al-espanol-de-la-csaguide-v3.0/>

<http://www.ismsforum.es/ficheros/descargas/csaguide-v2-1-es1353956041.pdf>

En esta tercera edición, a diferencia de en la segunda, cada dominio ha tenido un editor asignado, y ha contado con un equipo de revisores expertos. La estructura y numeración de los dominios concuerda con otros estándares de la industria y documentos de buenas prácticas. Recomendamos la adopción de estas guías como buenas prácticas para la gestión estratégica de los servicios soportados en *Cloud*. Esta documentación y sus fechas de publicación puede encontrarse en:

<http://www.cloudsecurityalliance.org/guidance/>

Respecto de la versión 2 del documento, se han actualizado los nombres de algunos dominios, en los dominios 3 (ahora "Cuestiones Legales: Contratos y eDISCOVERY") y 5 (ahora "Gestión de la Información y de la Seguridad de los Datos"). Se añade además un nuevo dominio, el Dominio 14, "Security as a Service".

© 2011 Cloud Security Alliance.

All rights reserved. You may download, store, display on your computer, view, print, and link to the Cloud Security Alliance Guidance at <http://www.cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf> subject to the following: (a) the Guidance may be used solely for your personal, informational, non-commercial use; (b) the Guidance may not be modified or altered in any way; (c) the Guidance may not be redistributed; and (d) the trademark, copyright or other notices may not be removed. You may quote portions of the Guidance as permitted by the Fair Use provisions of the United States Copyright Act, provided that you attribute the portions to the Cloud Security Alliance Guidance Version 3.0 (2011).

ÍNDICE

INTRODUCCIÓN	1
ÍNDICE	2
PRÓLOGO	3
AGRADECIMIENTOS	4
CARTA DE LOS EDITORES DE LA VERSIÓN EN INGLÉS	7
CARTA DEL CAPÍTULO ESPAÑOL, Y DE LOS EDITORES DE LA TRADUCCIÓN A ESPAÑOL	9
NOTA DE LOS EDITORES SOBRE RIESGOS	10
SECCIÓN I // ARQUITECTURA <i>CLOUD</i>	13
DOMINIO 1 //.....	14
MARCO DE REFERENCIA DE ARQUITECTURA PARA <i>CLOUD COMPUTING</i>	14
SECCIÓN II // GOBIERNO EN ENTORNO <i>CLOUD</i>	31
DOMINIO 2 //.....	32
GOBIERNO Y GESTIÓN DEL RIESGO CORPORATIVO	32
DOMINIO 3 //.....	38
CUESTIONES LEGALES: CONTRATOS Y eDISCOVERY	38
DOMINIO 4 //.....	47
CUMPLIMIENTO LEGAL Y GESTIÓN DE AUDITORÍA	47
DOMINIO 5 //.....	52
GESTIÓN DE LA INFORMACIÓN Y DE LA SEGURIDAD DE LOS DATOS	52
DOMINIO 6 //.....	66
INTEROPERABILIDAD Y PORTABILIDAD	66
SECTION III // OPERACIONES EN ENTORNO <i>CLOUD</i>	75
DOMINIO 7 //.....	76
SEGURIDAD TRADICIONAL, CONTINUIDAD DE NEGOCIO Y RECUPERACIÓN DE DESASTRES	76
DOMINIO 8 //.....	92
ACTIVIDADES DEL CPD	92
DOMINIO 9 //.....	96
RESPUESTA ANTE INCIDENTES	96
Domínio 10 //.....	107
SEGURIDAD DE APLICACIONES	107
DOMINIO 11 //.....	134
CIFRADO Y GESTIÓN DE CLAVES	134
DOMINIO 12 //.....	141
IDENTIDAD, ASIGNACIÓN DE DERECHOS, Y GESTIÓN DE ACCESOS	141
DOMINIO 13 //.....	163
VIRTUALIZACIÓN	163
DOMINIO 14 //.....	168
SECURITY AS A SERVICE	168
ANEXO A //.....	184
GLOSARIO EMPLEADO	184

PRÓLOGO

Bienvenidos a esta tercera versión de la “Guías de Seguridad de Áreas Críticas en *Cloud Computing*”, de la *Cloud Security Alliance* en su traducción a español. A medida que *Cloud computing* aumenta su madurez, la adecuada gestión de las oportunidades y retos en seguridad que implica *Cloud* supongo un elemento crucial para los procesos de negocio. Humildemente, esperamos que este documento aporte tanto orientación como inspiración para apoyar al negocio, mediante la gestión de los nuevos riesgos.

La *Cloud Security Alliance* ha proporcionado desde versiones anteriores de este documento buenas prácticas directamente aplicables. Es un proceso continuo de publicación de herramientas que permiten la transición de servicios a *Cloud* reduciendo los riesgos, del que este documento es referencia y orientación. En la versión 3.0 se recopilan datos y valoraciones recogidas de más de setenta expertos mundiales. La información proviene de un amplio rango de actividades, incluyendo los capítulos internacionales de CSA, socios, nuevas investigaciones y conferencias que permiten ampliar el alcance de los resultados y completar la misión de CSA. En www.cloudsecurityalliance.org puede tenerse información actualizada sobre las actividades de CSA.

El camino hasta conseguir que el *Cloud* sea seguro será largo, requerirá la participación de un conjunto de partes interesadas que cubran un punto de vista holístico. Sin embargo, debemos reconocer los progresos ya logrados: regularmente aparecen nuevas soluciones de seguridad *Cloud*, las compañías se apoyan en estas guías para contratar servicios *Cloud*, and se ha iniciado un enriquecedor debate a nivel mundial sobre aspectos de cumplimiento legal y confianza entre las partes en entornos *Cloud*. Pero el principal logro obtenido es que los profesionales de la seguridad están activamente implicados en hacer un futuro seguro, en lugar de conformarse con asegurar el presente.

Por favor, sigan estando implicados en este tema y continúen trabajando con nosotros para completar esta misión.

Cordiales saludos

Jerry Archer

Dave Cullinane

Nils Puhlmann

Alan Boehme

Paul Kurtz

Jim Reavis

Cloud Security Alliance Board of Directors

AGRADECIMIENTOS

De la Traducción a Español,

Realizada por el Capítulo Español de CSA (CSA-ES, <http://www.ismsforum.es/csa>)

Editores de la Edición Española

Mariano J. Benito, GMV

Antonio Sanz, Universidad de Zaragoza

Luis Buezo, HP

Nathaly Rey, ISMS Forum

Equipo de Traducción de la Edición Española

Enrique Aristi, Profesional Independiente

Roberto Baratta, NovaCaixaGalicia

Beatriz Blanco, KPMG

Mariano J. Benito, GMV

Diego Bueno, KPMG

Luis Buezo, HP

Ramses Gallego, QUEST a Dell Company

Ignacio Ivorra, Deloitte

Jorge Laredo, HP

Jaime Martin-Hinojal, Microsoft

Jose Leandro Núñez, Audens

Nathalie Rey, ISMS Forum

David Robles, Microsoft

Antonio Sanz, Universidad de Zaragoza

Equipo de Revisión de la Edición Española

Manuel Gómez, BT

Pedro López Peña, GMV

Antonio Ramos, Leet Security

Autores/Coautores de los Dominios, versión en inglés

Domain 1: Chris Hoff, Paul Simmonds

Domain 2: Marlin Pohlman, Becky Swain, Laura Posey, Bhavesh Bhagat

Domain 3: Francoise Gilbert, Pamela Jones Harbour, David Kessler, Sue Ross, Thomas Trappier

Domain 4: Marlin Pohlman, Said Tabet

Domain 5: Rich Mogull, Jesus Luna

Domain 6: Aradhna Chetal, Balaji Ramamoorthy, Jim Peterson, Joe Wallace, Michele Drgon, Tushar Bhavsar

Domain 7: Randolph Barr, Ram Kumar, Michael Machado, Marlin Pohlman

Domain 8: Liam Lynch

Domain 9: Michael Panico, Bernd Grobauer, Carlo Espiritu, Kathleen Moriarty, Lee Newcombe, Dominik Birk, Jeff Reed

Domain 10: Aradhna Chetal, Balaji Ramamoorthy, John Kinsella, Josey V. George, Sundararajan N., Devesh Bhatt, Tushar Bhavsar

Domain 11: Liam Lynch

Domain 12: Paul Simmonds, Andrew Yeomans, Ian Dobson, John Arnold, Adrian Secombe, Peter Johnson, Shane Tully, Balaji Ramamorthy, Subra Kumaraswamy, Rajiv Mishra, Ulrich Lang, Jens Laundrup, Yvonne Wilson

Domain 13: Dave Asprey, Richard Zhao, Kanchanna Ramasamy Balraj, Abhik Chaudhuri, Melvin M. Rodriguez

Domain 14: Jens Laundrup, Marlin Pohlman, Kevin Fielder

Equipo de Revisión, versión en Inglés

Valmiki Mukherjee, Bernd Jaeger, Ulrich Lang, Hassan Takabi, Pw Carey, Xavier Guerin, Troy D. Casey, James Beadel, Anton Chuvakin, Tushar Jain, M S Prasad, Damir Savanovic, Eiji Sasahara, Chad Woolf, Stefan Pettersson, M S Prasad, Nrupak Shah, Kimberley Laris, Henry St. Andre, Jim Peterson, Ariel Litvin, Tatsuya Kamimura, George Ferguson, Andrew Hay, Danielito Vizcayno,

K.S. Abhiraj, Liam Lynch, Michael Marks, JP Morgenthal, Amol Godbole, Damu Kuttikrishnan, Rajiv Mishra, Dennis F. Poindexter, Neil Fryer, Andrea Bilobrk, Balaji Ramamoorthy, Damir Savanovic

Equipo de Editores, versión en inglés

Archie Reed: Domains 3, 8, 9

Chris Rezek: Domains 2, 4, 5, 7, 13, 14

Paul Simmonds: Domains 1, 6, 10, 11, 12

CSA Staff

Technical Writer/Editor: Amy L. Van Antwerp

Graphic Designer: Kendall Scoboria

Research Director: J.R. Santos

CARTA DE LOS EDITORES DE LA VERSIÓN EN INGLÉS

En los últimos tres años, la *Cloud Security Alliance* ha incorporado a cerca de 120 nuevos socios corporativos y se ha volcado en tratar todos los aspectos de la seguridad *Cloud*, incluyendo el cumplimiento legal, legislación y regulaciones a nivel mundial en materia de seguridad, gestión de identidades, y los retos que suponen la monitorización y la auditoría de seguridad en una cadena de proveedores mundial basada en *Cloud*.

CSA se posiciona como una incubadora de estándares de seguridad en *Cloud*, de forma que los proyectos de investigación utilizan metodologías ágiles para la rápida producción de resultados. Para ello, el equipo editorial del documento de Guías presenta con orgullo la tercera versión de su documento fundamental “Guías de Seguridad de Áreas Críticas en *Cloud Computing*”. Este trabajo es un conjunto de las mejores prácticas de seguridad que CSA ha reunido en los 14 dominios involucrados en el gobierno y las operaciones en *Cloud*: Marco de Referencia de Arquitectura para *Cloud Computing*; Gobierno y Gestión del Riesgo Corporativo; Cuestiones Legales: Contratos y eDISCOVERY; Cumplimiento Legal y Gestión de Auditoría; Gestión de la Información y de la Seguridad de los Datos; Interoperabilidad y Portabilidad; Seguridad Tradicional; Continuidad de Negocio y Recuperación de Desastres; Actividades del CPD; Respuesta ante Incidentes; Seguridad de Aplicaciones; Cifrado y Gestión de Claves; Identidad, Asignación de Derechos y Gestión De Accesos; Virtualización ; y *Security as a Service*.

En esta tercera versión, las guías buscan establecer una base estable y segura para la operación en *Cloud*. Este esfuerzo proporciona un *roadmap* práctico y aplicable para los gestores que quieren adoptar soluciones *Cloud* con seguridad. SE han rescrito los dominios para hacer énfasis en la seguridad, estabilidad y la privacidad, asegurando la confidencialidad de la información corporativa en un entorno multi-tenancy.

En los últimos años, la versión 2.1 del documento ha sido la base para la investigación en múltiples áreas de la seguridad *Cloud*. Algunos entregables ya en aplicación, desde la “Arquitectura TCI” a la “Pila GRC”, se apoyan en las versiones previas de la guía, y esperamos que esto ocurra también para esta versión. Estas guías sirven como introducción de alto nivel para Directores ejecutivos, consumidores e implementadores que desean adoptar *Cloud computing* como una alternativa o como complemento a las arquitecturas TI tradicionales. No obstante, la guía se ha diseñado con espíritu innovador. Aquellos con un pensamiento más emprendedor pueden leer la guía con un ojo en los servicios y enfoques que los autores han deslizado y sugerido en ella. Para los inversores y los directores corporativos la guía les resultará interesante en tanto *roadmap* de investigación y desarrollo que ya está siendo usado en todo el mundo. Los responsables de seguridad e instructores encontrarán elementos que asientan conceptos, aunque provocadores. Y a medida que la industria evoluciona, el valor proporcionado por los autores se mostrará tan adecuado como influyente.

En esta tercera edición, las guías maduran en paralelo con el desarrollo de los estándares internacionales en el área, tanto en estructura como en contenidos. La versión 3.0 amplía los contenidos de versiones anteriores con requisitos y recomendaciones que pueden ser medidos y auditados. Por favor, se consciente de las diferentes interpretaciones que el término “requisitos” emplea a lo largo del documento. Estas guías no son de obligado cumplimiento, sino que “requisitos” representa las guías adecuadas para, virtualmente, cubrir todos las situaciones que pudimos prever, y también alinea las guías con otros documentos aceptados por la industria. Los expertos de la industria que participan en CSA han trabajado para presentar un producto usable, que considera y equilibra los intereses de los proveedores de servicios *Cloud* y los usuarios. Los controles se enfocan en preservar la integridad de la propiedad de los datos de los usuarios, apoyando a la vez el uso de infraestructuras físicas compartidas. La versión 3 de las Guías asume la naturaleza altamente dinámica del *Cloud*, la curva de aprendizaje y el desarrollo de nuevos productos como la CCM (*Cloud Controls Matrix*), CAI (*Consensus Assessments Initiative*), TCI (*Trusted Cloud Initiative*) y GRC Stack, y agrupa las actividades de

CSA en un único documento ejecutivo. Las Guía V3.0 servirán como la puerta de entrada para los estándares emergentes que se están desarrollando por organizaciones a nivel mundial, y está diseñado para que sirva como un primer elemento a nivel ejecutivo para cualquier organización que busque una transición segura y estable para migrar sus operaciones de negocio en el *Cloud*.

De parte de la *Cloud Security Alliance*, querríamos agradecer a todos y cada uno de los voluntarios por su tiempo y dedicación para el desarrollo y edición de esta nueva versión de nuevo documento fundamental. Creemos que este es nuestro mejor y más completo trabajo hasta la fecha, si bien el tema sigue evolucionando y, aunque nuestra idea fundamental es orientar, también pretendemos motivar a los lectores para que aporten ideas y mejoras en la línea que perfila el documento. Humildemente, publicamos este trabajo para la industria y esperamos su aportación más importante al diálogo, sus opiniones. Estamos deseosos de recibir sus opiniones sobre estas Guías. Si encuentra que las Guías son útiles, o quisiera mejorarlas de cualquier forma, valora la posibilidad de unirse a la *Cloud Security Alliance*, tanto como miembro como colaborador.

¡Saludos!

Paul Simmonds

Chris Rezek

Archie Reed

Security Guidance v3.0 Editors

CARTA DEL CAPÍTULO ESPAÑOL, Y DE LOS EDITORES DE LA TRADUCCIÓN A ESPAÑOL

Para el Capítulo Español de la Cloud Security Alliance, es motivo de gran satisfacción poder presentar la traducción a lengua española del documento fundamental de trabajo de la CSA, este “Guías de Seguridad de Áreas Críticas en *Cloud Computing*”, en versión 3.

Esta Guía es la mejor y más completa referencia a nivel internacional sobre las medidas de seguridad y aspectos a tener en cuenta que pueden aplicar las organizaciones que desean apoyarse en los servicios que ofrecen *Cloud* o que desean migrar sus servicios TI actuales a ella. La iniciativa de traducir este documento tiene como objetivo fundamental poner a disposición de toda la comunidad hispanohablante este documento clave para la segura adopción del *Cloud*, facilitando sus contenidos por encima de las barreras que pudiera suponer el idioma, y promoviendo el uso de la terminología propia en español.

Desde el capítulo queremos agradecer a nuestros compañeros del Comité Técnico de Organización del CSA-ES y a los socios que han participado en estas tareas, con la participación adicional de expertos en Cloud, seguridad y proveedores de servicio y usuarios finales, contando con la colaboración de expertos de las compañías Audens, BT, Dell, Deloitte, GMV, HP, ISACA, KPMG, Microsoft, NovaCaixaGalicia, Universidad de Zaragoza y expertos independientes.

NOTA DE LOS EDITORES SOBRE RIESGOS

A lo largo de todo el documento, se hacen frecuentes recomendaciones para reducir los riesgos derivados de la adopción del *Cloud*, pero no todas estas recomendaciones son necesarias o incluso realistas para todos los despliegues *Cloud*. Dado que se ha recopilado información de diferentes grupos durante el proceso de edición, rápidamente fue evidente que simplemente no había espacio en el documento para dar recomendaciones completas para todos los posibles escenarios de riesgo. Igual que una aplicación crítica puede ser simplemente demasiado importante para llevarla a un proveedor *Cloud* público, los controles de seguridad para datos poco relevantes en un servicio de almacenamiento *Cloud* deben ser también poco relevantes.

Ante la gran variedad de opciones de despliegues de *Cloud* (tanto SaaS, PaaS o IaaS; pública o privada; alojamiento interno y externo y diversos híbridos de todos ellos), ningún conjunto de controles de seguridad pueden cubrir cualquier tipo de circunstancias. Y como en cualquier otra situación, las organizaciones deberían adoptar una estrategia de migración a *Cloud* basada en análisis de riesgos. A continuación, se muestra un marco de referencia sencillo que puede ayudar a hacer una evaluación de riesgos preliminar y tomar decisiones de seguridad adecuadas.

Este proceso no es un proceso completo de análisis de riesgos, ni una metodología para identificar todos los requisitos de seguridad. Se trata de un método rápido para determinar la viabilidad del movimiento de un activo a alguno de los modelos de *Cloud*.

Identificar los Activos que se quieren desplegar en *Cloud*

Simplificando, los activos que se pueden migrar a *Cloud* pueden ser de dos tipos:

1. Datos
2. Servicios, aplicaciones, funcionalidades o procesos

Puesto que se están moviendo a *Cloud* información o transacciones/procesado de datos (desde operaciones concretas hasta aplicaciones completas)

En un servicio *Cloud*, no es imprescindible que los datos y las aplicaciones residan en la misma ubicación, y se puede optar por mover a *Cloud* parte de las funciones. Por ejemplo, podemos albergar la aplicación y los datos en un CPD local, y además externalizar parte de sus funcionalidades a un *Cloud* tipo PaaS.

El primer paso en la evaluación del riesgo *Cloud* es determinar con precisión que datos y funcionalidades se está considerando mover. Incluyendo en su caso usos adicionales que pudieran aparecer una vez migrados los datos. Debe considerarse también que el volumen de tráfico, datos y operaciones son, en ocasiones, mayores de lo esperado.

Valorar los activos

El siguiente paso es determinar cuan importantes son las operaciones y/o datos para la organización. No es necesario hacer una evaluación detallada, salvo que la organización tenga un proceso formal para ellos, pero si es necesaria una valoración aun de trazo grueso sobre cuan confidencial es la información y cuan importante es el proceso, operación o función.

Para ello, hágase las siguientes preguntas.

1. ¿En qué forma se dañaría a la organización si el activo estuviera públicamente accesible y disponible?
2. ¿En qué forma se dañaría a la organización si un empleado del proveedor de *Cloud* accediera al activo?
3. ¿En qué forma se dañaría a la organización si el proceso fuera alterado por alguien externo?
4. ¿En qué forma se dañaría a la organización si el proceso o función no proporcionase los resultados esperados?
5. ¿En qué forma se dañaría a la organización si la información o los datos se alterasen de forma inesperada?
6. ¿En qué forma se dañaría a la organización si el activo no estuviera disponible durante un tiempo?

Esencialmente, estas preguntas sirvan para valorar el activo en sus necesidades de confidencialidad, integridad y disponibilidad, y como el riesgo varía si el activo se lleva total o parcialmente a *Cloud*. Es un proceso similar a una valoración de un proyecto de externalización, salvo en que en *Cloud* hay muchas más opciones de trabajo, incluyendo entre ellas los modelos de trabajo en la propia organización tradicionales.

Valorar el activo en los distintos modelos de despliegue *Cloud*

En estos momentos, ya se debe entender la importancia del activo. El siguiente paso es identificar los modelos de despliegue que mejor se ajustan. Antes de buscar posibles proveedores de servicio, deberíamos conocer si los riesgos de los distintos modelos son aceptables: público, privado, comunitarias o híbridas; y escenarios de alojamiento: interno, externo o combinado.

Para ello, identifica si para este activo, serían aceptables las siguientes opciones:

1. Público
2. Privado, pero interno o en instalaciones propias.
3. Privado, pero externo (incluyendo infraestructuras dedicadas o compartidas)
4. Comunitarias, teniendo en cuenta la ubicación de las infraestructuras, potenciales proveedores el resto de los miembros de la comunidad.
5. Híbrido, Para evaluar con precisión esta opción hay que tener en cuenta al menos una idea sobre la arquitectura que albergará los componentes, funciones y datos.

En este punto, debería disponerse de una idea suficiente de cuan cómodo se encuentra la organización con una migración a *Cloud*, y los modelos y ubicaciones que se adaptan a los requisitos de riesgo y seguridad.

Valorar los potenciales modelos de servicios y proveedores *Cloud*

Este paso se enfoca en el grado de control que se dispondrá en cada nivel de servicio *Cloud*, para implantar medidas de control del riesgo. Si se está evaluando una propuesta concreta, posiblemente sea necesario hacer un análisis de riesgos más completo.

El foco ha de ser el grado de control de que se dispondrá en cada nivel para mitigar los riesgos. Si se dispone de requisitos precisos (legales, contractuales), es el momento de incluirlos en la evaluación.

Describe los flujos de datos

Si se está evaluando un despliegue específico, han de describirse los flujos de datos entre la organización, el servicio *Cloud*, los clientes y otros actores que intervengan. Aunque gran parte de esta descripción ya se debería haber hecho en fases anteriores, es completamente esencial entender si los datos se mueven a *Cloud* y como se hace este movimiento antes de tomar una decisión final.

Si se ha de tomar una decisión sobre una oferta particular, deberías describir los datos para todas las opciones que se están manejando. Así, se puede estar seguro de todos los riesgos a los que se exponen los datos antes de tomar una decisión final.

Conclusiones

Con este proceso, se debería entender la importancia de los elementos que se quieren mover al *Cloud*, la tolerancia al riesgo de este movimiento, y las posibilidades de despliegues y modelos de servicio que son aceptables. Y una idea muy cercana a la realidad de los riesgos a los que se está exponiendo los datos.

Todo ello junto debería constituir información de contexto suficiente para evaluar cualquier control de seguridad contenido en este documento. Para activos de baja importancia, no se necesita un alto grado de seguridad y pueden obviarse muchas de las recomendaciones (inspecciones en el proveedor, cifrado complejo, eDiscovery, ...). Un activo de alto valor y sometido a regulación podría requerir la generación de trazas de auditoría y una política de conservación de estas trazas. Un activo de alto valor y sin requisitos de regulación puede requerir mayor cantidad e intensidad de controles de seguridad de tipo técnico

Debido a las limitaciones de espacio, y a la profundidad de las materias cubiertas, este documento contiene una extensa lista de recomendaciones de seguridad. No en todos los casos será necesario aplicar todos los controles de seguridad y gestión de riesgos posibles. Dedicar algo de tiempo para evaluar la tolerancia al riesgo y la exposición al mismo proporciona la información que se necesita para elegir las mejores opciones para cada organización y despliegue.



SECCIÓN I //
ARQUITECTURA
CLOUD

DOMINIO 1 //

MARCO DE REFERENCIA DE ARQUITECTURA PARA *CLOUD COMPUTING*

Este dominio, “Marco de Referencia de arquitectura para *Cloud Computing*”, proporciona un marco conceptual para el resto de la guía de *Cloud Security Alliance*. El contenido de este dominio se focaliza en una descripción de *Cloud computing* específicamente adaptada a la perspectiva concreta de los profesionales de seguridad y de redes TI. La sección final de este dominio proporciona una breve introducción a cada uno de los dominios restantes.

Entender el Marco de Referencia descrito en el presente dominio es un paso importante para el entendimiento del resto de la guía del *Cloud Security Alliance*. Dicho marco, define muchos de los conceptos y términos usados a lo largo de los otros dominios implicados.

Introducción. Las siguientes tres secciones definen la perspectiva de la arquitectura en términos de:

- Terminología usada a lo largo de la guía al objeto de proporcionar un léxico consistente.
- Los requisitos de arquitectura y retos de seguridad para las aplicaciones y los servicios *Cloud*.
- Un modelo de referencia que describa una taxonomía de servicios y arquitecturas *Cloud*.

1.1 ¿Qué es el *Cloud Computing*?

Cloud computing es un modelo para proporcionar acceso ubicuo, conveniente y bajo demanda a un conjunto de recursos de computación configurable (p. ej., redes, servidores, almacenamiento, aplicaciones y servicios). *Cloud Computing* es una tecnología puntera que tiene el potencial de mejorar la colaboración, la agilidad, la escalabilidad y la disponibilidad así como de proporcionar oportunidades de reducción de costes a través de una computación optimizada y eficiente. El modelo *Cloud Computing* prevé un mundo donde los componentes puedan ser orquestados, aprovisionados, implementados y des-aprovisionados con rapidez, así como escalados hacia arriba y hacia abajo con el objeto de proporcionar un modelo de distribución y consumo bajo demanda parecido al de los servicios públicos.

Desde el punto de vista de la arquitectura, hay mucha confusión en torno a cómo el *Cloud* es a la vez similar y diferente a los modelos existentes de computación, y de cómo estas similitudes y diferencias influyen en los enfoques organizativos, operativos y tecnológicos de las prácticas de seguridad y redes TI. Hay una fina línea divisoria entre computación convencional y computación en *Cloud*. No obstante, el *Cloud computing* influirá sobre los enfoques organizacionales, operativos y tecnológicos en relación a las buenas prácticas de aseguramiento de datos, redes y la seguridad de la información en general.

Hoy por hoy, hay muchas definiciones que intentan abordar *Cloud* desde una perspectiva académica, de arquitectura, ingenieril, para desarrolladores, gerentes y/o usuarios. Este documento se focaliza en una definición específicamente adaptada a la perspectiva concreta de los profesionales de seguridad y redes TI.

1.2 ¿En qué consiste el *Cloud Computing*?

Esta versión de la guía de *Cloud Security Alliance* cuenta con las definiciones basadas en los trabajos publicados por los científicos del *National Institute of Standards and Technology* (en adelante NIST) y sus esfuerzos en torno a la definición del *Cloud computing*.

Por regla general, la publicación del NIST es bien aceptada, y esta guía se alinea con el *Working Definition of Cloud Computing* de NIST (en adelante NIST 800-145) para dar coherencia y consenso en torno a un lenguaje común, y centrarse en los casos de uso en lugar de centrarse en los matices semánticos.

Es importante observar que esta guía está destinada a ser ampliamente utilizable y globalmente aplicable a las organizaciones. Mientras el NIST es una organización gubernamental de E.E.U.U., la selección de este modelo de referencia no debería interpretarse como una sugerencia de exclusión de otros puntos de vista o áreas geográficas.

El NIST define *Cloud computing* mediante la descripción de cinco características esenciales, tres modelos de servicio en *Cloud* y cuatro modelos de despliegue para *Cloud*. En la Figura 1 se resumen de forma visual y se explica en detalle a continuación.

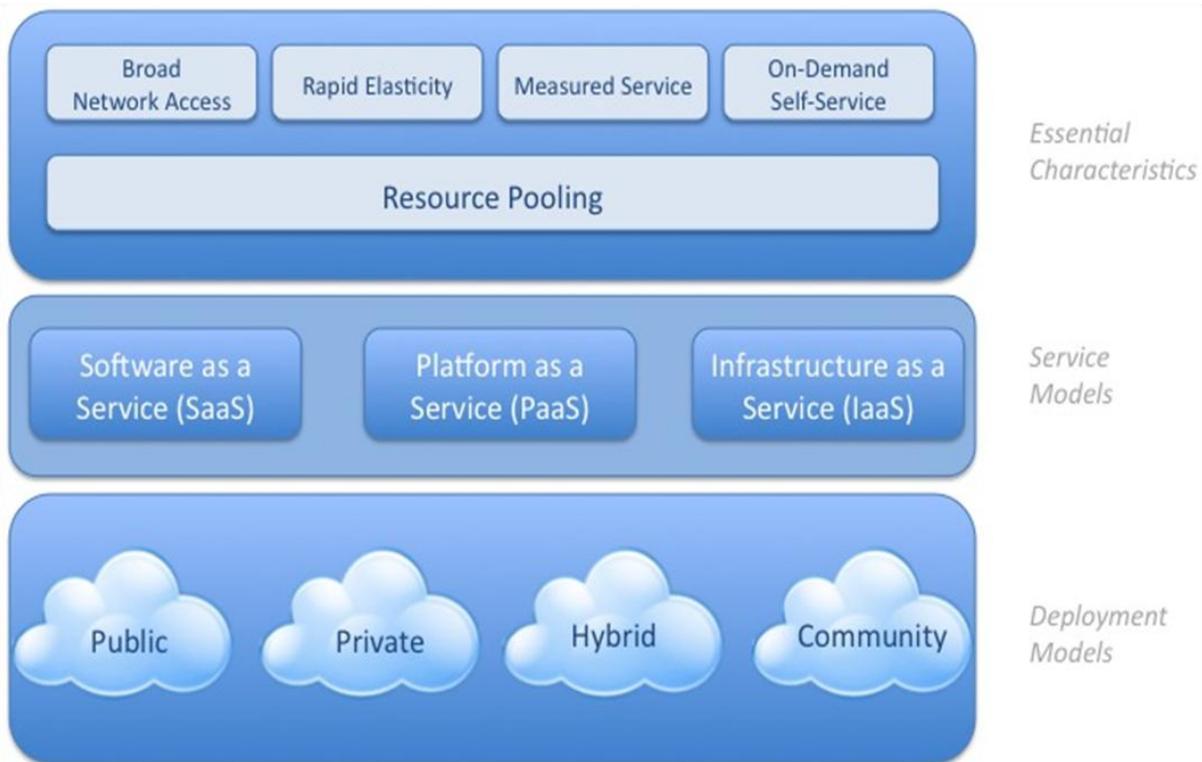


Figura 1—Modelo visual de la definición de *Cloud Computing* según NIST

1.3 Las características del *Cloud Computing*

Es importante reconocer que los servicios *Cloud* son a menudo, pero no siempre, utilizados en conjunción con y habilitados por las tecnologías de virtualización. Sin embargo, no hay ningún requisito que aúne la abstracción de

recursos con las tecnologías de virtualización y en muchas propuestas no se utiliza la virtualización por el hipervisor o el contenedor del sistema operativo.

Además, debe tenerse en cuenta que *multi-tenancy* no es una característica esencial de *Cloud* según el NIST, pero a veces se discute como si lo fuera. CSA ha identificado *multi-tenancy* como un elemento importante del *Cloud*.

1.4 Multi-Tenancy

Como se ha señalado antes, en este documento, *multi-tenancy* se considera un elemento importante, y en la siguiente sección se perfilará como un elemento importante del *Cloud computing* conforme la comprensión y definición de CSA.

En su forma más simple, *multi-tenancy* implica el uso de los mismos recursos o aplicaciones por parte de múltiples clientes que pueden pertenecer a la misma organización o a organizaciones diferentes. En materia de seguridad, los riesgos de *multi-tenancy* se encuentran en la visibilidad de los datos entre clientes o la visibilidad en el seguimiento de las operaciones de otro usuario o inquilino.

En los modelos de servicio en el *Cloud*, *multi-tenancy* implica la necesidad de una política impulsada por la segmentación, el aislamiento, el gobierno, los niveles de servicio y los modelos de facturación por consumo para diferentes clientes.

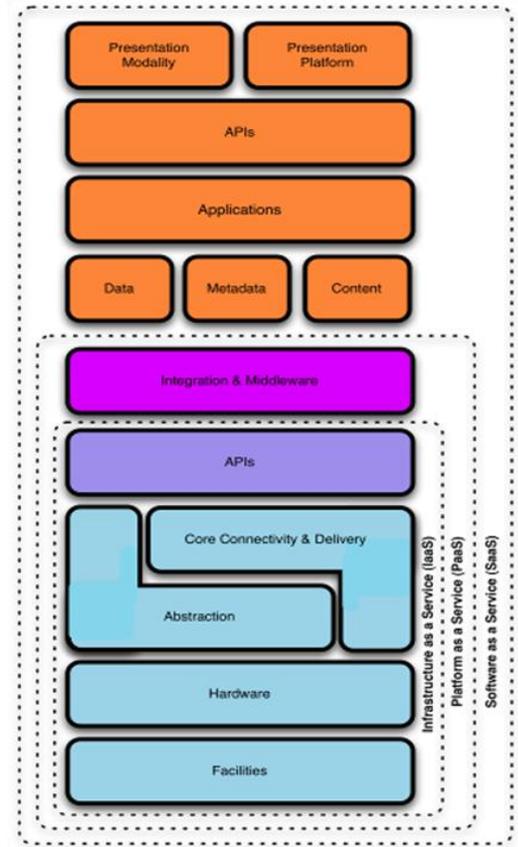
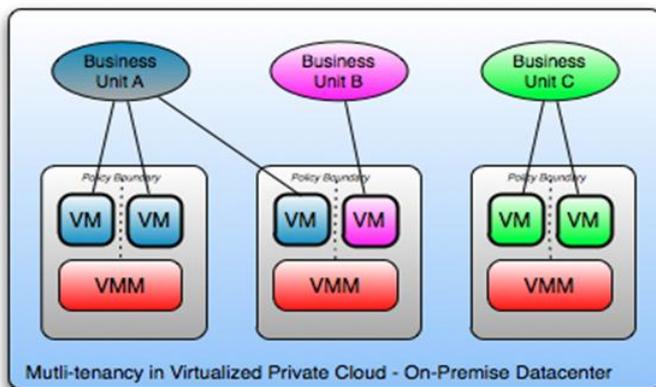
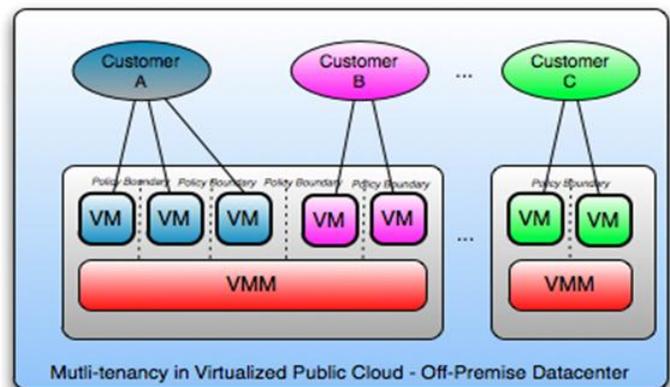


Figura 2a —Multi-Tenancy



Private Cloud of Company XYZ with 3 business units, each with different security, SLA, governance and chargeback policies on shared infrastructure



Public Cloud Provider with 3 business customers, each with different security, SLA, governance and billing policies on shared infrastructure

Figura 2b—Multi-Tenancy

Los usuarios pueden optar por utilizar un servicio *Cloud* de un proveedor público ofrecido a usuarios individuales uno a uno o, en el caso de alojamiento privado en *Cloud*, una organización puede segmentar sus usuarios como unidades de negocio diferentes que comparten una infraestructura común.

Desde la perspectiva del proveedor, el *multi-tenancy* sugiere un enfoque de arquitectura y de diseño que habilite economías de escala, disponibilidad, gestión, segmentación, aislamiento y eficiencia operativa. Estos servicios aprovechan la infraestructura, datos, metadatos, servicios y aplicaciones que son compartidos por muchos usuarios diferentes.

Multi-tenancy también puede asumir diferentes definiciones, dependiendo del modelo de servicio *Cloud* del proveedor, en la medida en que pueda suponer la habilitación de las capacidades descritas anteriormente en relación a la infraestructura, la base de datos o los niveles de aplicación. Un ejemplo podría ser la diferencia entre *Infrastructure-as-a-Service (IaaS)*, *Software-as-a-Service (SaaS)* y *Platform-as-a-Service (PaaS)* a la hora de llevar a cabo una implementación *multi-tenant*.

La implementación de cada modelo da una importancia diferente a *multi-tenancy*. Sin embargo, incluso en el caso de *Cloud* privado, una única organización puede tener un gran número de consultores y contratistas, así como el deseo de un alto grado de separación lógica entre unidades de negocio. Así las cosas, los aspectos a valorar relacionados con *multi-tenancy* deben ser siempre tenidos en cuenta.

1.5 Modelo de Referencia *Cloud*

Entender las relaciones y dependencias entre los modelos de *Cloud computing* es fundamental para comprender los riesgos asociados a la seguridad. *IaaS* es la base de todos los servicios *Cloud*, con *PaaS* basándose en *IaaS* y *SaaS*, a su vez, construido sobre *PaaS* como se describe en el diagrama del Modelo de Referencia del *Cloud*. De esta manera, al igual que se heredan las capacidades, también se heredan los aspectos y los riesgos relativos a la seguridad de la información. Es importante señalar que los proveedores comerciales de *Cloud* puede que no encajen perfectamente en los modelos de servicio por capas. Sin embargo, el modelo de referencia es importante para relacionar los servicios del mundo real con un Marco de Referencia de arquitectura, y para entender que los recursos y servicios requieren de un análisis de seguridad.

IaaS incluye una pila completa de recursos de infraestructura, desde las instalaciones hasta las plataformas hardware que residen en ellas. Incorpora la capacidad de abstraer recursos (o no), así como la de proporcionar una conectividad física y lógica a dichos recursos. En última instancia, *IaaS* proporciona un conjunto de **APIs**¹, que permiten la gestión y otro tipo de interacciones por parte de los usuarios con la infraestructura.

Infrastructure as a Service (IaaS), ofrece una infraestructura computacional (normalmente un entorno de virtualización de plataforma) como un servicio, junto con almacenamiento puro y gestión de la red. En lugar de comprar servidores, software, espacio en el CPD, o equipos de red, los clientes compran esos recursos como un servicio totalmente externalizado.

Software as a Service (SaaS), a veces referido como "software bajo demanda", es un modelo de entrega de software en el que se alojan el software y sus datos asociados centralizadamente (Normalmente en *Cloud* (Internet)) y el acceso por los usuarios se realiza usando un cliente ligero, normalmente un navegador web.

Platform as a service (PaaS), es la entrega de una plataforma de computación y de una pila de soluciones como un servicio. *PaaS* ofrece facilitar el despliegue de aplicaciones sin el coste y la complejidad de comprar y gestionar el hardware y el software subyacentes, así como las capacidades de aprovisionamiento del alojamiento. Esto proporciona todos los servicios necesarios para soportar el ciclo de vida completo de la creación y entrega de aplicaciones y servicios web

¹ API - Application Programming Interface (Interfaz de Programación de Aplicaciones)

PaaS se coloca por encima de IaaS y añade una capa adicional de integración con los marcos de referencia de desarrollo de aplicaciones, capacidades de middleware y funciones como bases de datos, mensajería y gestión de colas. Estos servicios permiten a los desarrolladores crear aplicaciones en la plataforma con los lenguajes de programación y herramientas soportados por la pila.

A su vez, SaaS se basa en las pilas subyacentes IaaS y PaaS, ofreciendo un entorno operativo independiente que es utilizado para proporcionar la experiencia de usuario de forma completa, incluyendo el contenido, su presentación, la(s) aplicación(s) y las capacidades de gestión.

Por lo tanto, debería quedar claro que cada modelo presenta importantes ventajas y desventajas en términos de características integradas, de complejidad frente a apertura (o capacidad de ser extendido) y de seguridad. Por regla general, SaaS proporciona la mayor funcionalidad integrada directamente en la oferta, con la menor extensibilidad de usuario y un nivel de seguridad integrado relativamente alto (como mínimo, la seguridad es responsabilidad del proveedor).

PaaS está destinado a permitir a los desarrolladores construir sus propias aplicaciones en la parte superior de la plataforma. Como resultado, tiende a ser más extensible que SaaS a expensas de proporcionar menos funcionalidades ya preparadas para el cliente. Este equilibrio se extiende a las funciones y capacidades de seguridad donde las capacidades integradas son menos completas, pero hay más flexibilidad para añadir niveles de seguridad adicional.

IaaS ofrece pocas, sino ninguna, características de aplicación pero sí una extensibilidad enorme. En general, esto significa menos capacidades integradas de seguridad y menos funcionalidad más allá de la protección de la propia infraestructura. Este modelo requiere que los sistemas operativos, las aplicaciones y el contenido sean gestionados y securizados por el usuario del *Cloud*.

La conclusión clave para la arquitectura de seguridad es que cuanto más abajo se detiene la pila del proveedor de servicios *Cloud*, mayor es la responsabilidad de los usuarios en materia de implementación y gestión de las capacidades de seguridad que deberán realizar por ellos mismos.

Los niveles de servicio, la seguridad, el gobierno, el cumplimiento legal y las expectativas de responsabilidad del servicio y del proveedor se estipulan, gestionan y aplican contractualmente cuando se ofrece al usuario un acuerdo de nivel de servicio (**ANS** o **SLA**)². Hay dos tipos de SLA: los negociables y los no negociables. En ausencia de un SLA, el usuario administra todos los aspectos del *Cloud* bajo su control. Cuando se ofrece un SLA no negociable, el proveedor administra las partes estipuladas en el acuerdo. Por regla general, en los casos de PaaS o de IaaS es responsabilidad de los administradores de sistemas del usuario la gestión eficaz de los servicios residuales especificados en el ANS, con alguna compensación por parte del proveedor al objeto de securizar la plataforma subyacente y los componentes de infraestructura de forma que se garantice la disponibilidad y la seguridad del servicio. Debe quedar claro en todos los casos que se pueden asignar / transferir la responsabilidad pero no necesariamente quien asume las consecuencias.

Acotando el alcance o algunas capacidades y funcionalidades específicas dentro de cada uno de los modelos de entrega del *Cloud*, o bien empleando la asociación funcional de servicios y capacidades a través de ellos, se pueden producir clasificaciones derivadas. Por ejemplo, "Storage as a Service" es una sub-oferta dentro de la "familia" IaaS.

Mientras que una revisión más amplia del conjunto cada vez mayor de soluciones de *Cloud computing* está fuera del alcance de este documento, el "OpenCrowd Cloud Solutions taxonomy" de la siguiente figura proporciona un excelente

² **ANS** (Acuerdo de Nivel de Servicio) o **SLA**-(Service Level Agreement)

punto de partida. Sin embargo, específicamente CSA no prescribe ninguna de las soluciones o empresas que se muestran más abajo. Se proporciona el diagrama para mostrar la diversidad de ofertas disponibles en la actualidad.

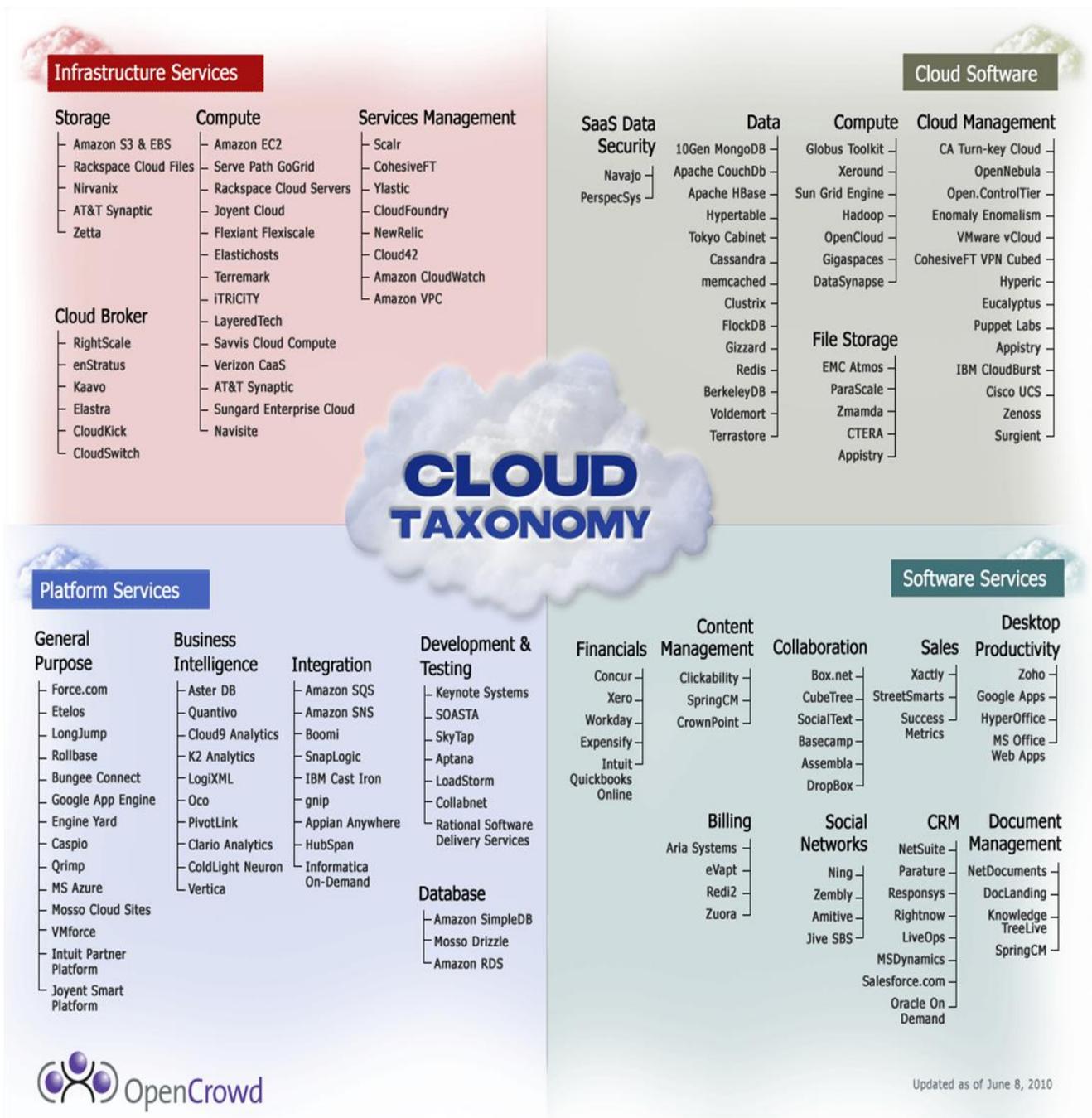


Figura 3 – Taxonomía del OpenCrowd³

Para una excelente revisión de los muchos casos de uso de *Cloud computing*, el *Cloud Computing Use Case Group* creó un grupo de trabajo colaborativo con el fin de describir y definir los casos comunes y demostrar los beneficios del *Cloud*, siendo su meta "... reunir a los usuarios y fabricantes de *Cloud* para definir los casos de uso común del *Cloud*

³ http://www.opencrowd.com/assets/images/views/views_cloud-tax-lrg.png

computing... y poner de relieve las capacidades y los requisitos que deben estandarizarse en un entorno de *Cloud* para garantizar la interoperabilidad, la facilidad de integración y la portabilidad."

1.5.1 Modelo de referencia de seguridad *Cloud*

El modelo de referencia de seguridad de *Cloud* trata las relaciones de estas tipologías y las coloca en el contexto de sus controles y aspectos a valorar relevantes en materia de seguridad. Para las organizaciones y las personas que lidian con *Cloud computing* por primera vez, es importante tener en cuenta lo siguiente para evitar posibles dificultades y confusiones:

- La noción de *cómo* se implementan los servicios *Cloud* a menudo se utiliza de forma intercambiable con el lugar donde se prestan dichos servicios, lo que puede llevar a confusión. *Cloud* públicos o privados pueden ser descritos como externos o internos, lo que puede no ser exacto en cualquier situación.
- A menudo, la manera en que los servicios *Cloud* se describe en relación a la ubicación de la gestión de una organización o al perímetro de seguridad (por lo general, se define por la presencia de un *demarc* conocido). Y mientras es importante entender el alcance de los servicios que están en *Cloud* para entender dónde se encuentran los límites de seguridad en cuanto a *Cloud computing* se refiere, no ha de confundirse con la noción de un perímetro de seguridad, que es un concepto anacrónico para la mayoría de las organizaciones.
- El *Cloud computing* amplifica y acelera la re-perimetrización y la erosión de los límites de confianza, algo que ya está sucediendo en las empresas. La conectividad ubicua, los múltiples intercambio de información y la ineficacia de los controles estáticos de seguridad tradicionales que no puede hacer frente a la naturaleza dinámica de los servicios *Cloud*, hacen requerir un nuevo pensamiento en relación a *Cloud computing*. El *Jericho Forum*⁴ ha producido una cantidad considerable de material sobre la re-perimetrización de las redes empresariales, incluyendo muchos casos de estudio.

Las modalidades de despliegue y uso de *Cloud* deben ser pensadas no sólo dentro del contexto "interno" frente al "externo" en lo que respecta a la ubicación física de los activos, los recursos y la información, sino también por quienes están siendo usados, así como quién es responsable de su gobierno, seguridad y cumplimiento con las políticas y estándares.

Esto no quiere decir que el hecho de que un activo, un recurso o la información estén ubicados dentro o fuera de las instalaciones no afecte a la seguridad y a la exposición al riesgo de una organización, porque sí que afecta, pero se pretende enfatizar que el riesgo también depende de:

- Los tipos de activos, recursos e información que están siendo gestionados
- Quién los gestiona y cómo
- Qué controles se han seleccionado y cómo han sido integrados
- Aspectos relacionados con el cumplimiento legal

⁴ <http://www.jerichoforum.org>

Por ejemplo, una pila **LAMP**⁵ desplegada en el AWS EC2 de Amazon sería clasificada como una solución pública IaaS gestionada por terceros fuera de las instalaciones, incluso si las instancias y aplicaciones / datos contenidos fueran gestionados por el usuario o un tercero. Una pila de aplicaciones personalizadas que da servicio a varias unidades de negocio desplegadas sobre *Eucalyptus* bajo el control, la gestión y la propiedad de una empresa, se podría describir como una solución privada SaaS autogestionada en sus instalaciones. Ambos ejemplos usan el escalado elástico y las capacidades de auto-servicio del *Cloud*.

La siguiente tabla resume los puntos de la siguiente tabla:

Tabla 1— Modelos de implementación del Cloud

	Infrastructure Managed By ¹	Infrastructure Owned By ²	Infrastructure Located ³	Accessible and Consumed By ⁴
Public	Third Party Provider	Third Party Provider	Off-Premise	Untrusted
Private/Community	Or Organization Third Party Provider	Organization Third Party Provider	On-Premise Off-Premise	Trusted
Hybrid	Both Organization & Third Party Provider	Both Organization & Third Party Provider	Both On-Premise & Off-Premise	Trusted & Untrusted

¹ Management includes: governance, operations, security, compliance, etc...
² Infrastructure implies physical infrastructure such as facilities, compute, network & storage equipment
³ Infrastructure Location is both physical and relative to an Organization's management umbrella and speaks to ownership versus control
⁴ Trusted consumers of service are those who are considered part of an organization's legal/contractual/policy umbrella including employees, contractors, & business partners. Untrusted consumers are those that may be authorized to consume some/all services but are not logical extensions of the organization.

Otra forma de visualizar las combinaciones de modelos de servicios, de modelos de despliegue, de ubicaciones físicas de los recursos y de la atribución de la gestión y la propiedad del *Cloud*, es el modelo del *Jericho Forum's Cloud Cube Model*⁶ que se muestra en la figura 4:

El *Cloud Cube Model* ilustra las muchas permutaciones disponibles hoy en ofertas de *Cloud* y presenta cuatro criterios / dimensiones con el fin de diferenciar unas "formaciones" de *Cloud* de otras y su forma de provisión, con el fin de entender cómo el *Cloud computing* afecta a la forma en que la seguridad podría ser abordada.

⁵ LAMP-Linux (sistema operativo), [Apache HTTP Server](#), [MySQL \(database software\)](#) y [Perl/PHP/Python](#), los principales componentes para construir un [web server](#) viable de propósito general

⁶ http://www.opengroup.org/jericho/cloud_cube_model_v1.0.pdf

El *Cloud Cube Model* también pone de relieve los desafíos de la comprensión y el mapeo de modelos de *Cloud* para controlar los marcos de referencia y estándares como la ISO / IEC 27002, que establece que "... una serie de directrices y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información dentro de una organización."

La ISO/IEC 27002, en su sección 6.2, establece como objetivos de control de "Partes externas": "... la seguridad de la información de la organización y las instalaciones de procesamiento de información no deben ser reducidas por la introducción de productos y servicios de terceros..."

Así las cosas, las diferencias existentes en los métodos y en las responsabilidades a la hora de securizar los tres modelos de servicios *Cloud* viene a decir que los usuarios de dichos servicios se enfrentan a una tarea complicada. A menos que los proveedores de *Cloud*

puedan de buena gana dar a conocer sus controles de seguridad y el grado en el que se implementan

para el usuario, y el usuario sepa qué controles son necesarios para mantener la seguridad de su información, hay un enorme potencial para decisiones erróneas en la gestión del riesgo así como para resultados perjudiciales.

En primer lugar, se clasifica un servicio *Cloud* por el modelo de arquitectura *Cloud*. Entonces, es posible mapear su arquitectura de seguridad, así como otros requisitos de negocio, regulatorios y de cumplimiento legal contra dicha estructura como si de un ejercicio de análisis GAP se tratara. El resultado determina la posición general de "seguridad" de un servicio y cómo se relaciona con la seguridad de un activo y los requisitos de protección.

La figura 5 muestra un ejemplo de cómo un servicio de *Cloud* puede ser comparado con un catálogo de controles compensatorios para determinar qué controles existen y cuáles no - conforme a lo dispuesto por el usuario, el proveedor de servicios de *Cloud* o un tercero. A su vez, puede ser comparado con un marco de referencia de cumplimiento legal o un conjunto de requisitos tales como PCI DSS, tal y como es mostrado.

Una vez que este análisis *GAP* se ha completado, de acuerdo a los requisitos de cualquier mandato regulatorio u otros mandatos de cumplimiento legal, se hace mucho más fácil determinar lo que es necesario hacer con el fin de retroalimentar un marco de referencia para la evaluación de riesgos. Esto, a su vez, ayuda a determinar cómo los *GAP* y, en última instancia los riesgos, deben ser abordados: mediante aceptación, transferencia o mitigación.

Es importante señalar que el uso de *Cloud computing* como modelo operativo no proporciona e cumplimiento legal o prevención de incumplimiento de forma intrínseca. La habilidad de cumplir con cualquier requisito es el resultado directo del modelo de servicio y del modelo de despliegue utilizado, así como del diseño, de la implementación y de la administración de los recursos dentro del alcance.

Para una completa revisión del marco de control, que incluye buenos ejemplos de la estructura de control genérica a la que se ha hecho referencia anteriormente, véase el panorama de documentación sobre patrones de arquitectura de

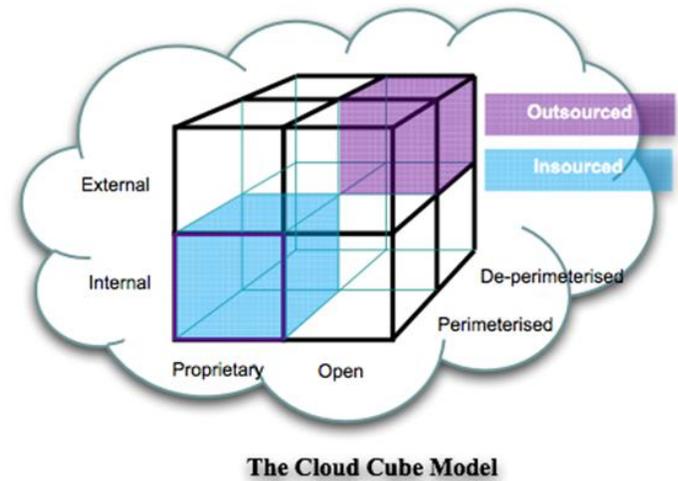


Figura 4—Jericho Cloud Cube Model

seguridad del *Open Security Architecture Group's*⁷, o la siempre útil y recientemente actualizada NIST 800-53 revisión 3 sobre Controles de Seguridad Recomendados para Sistemas de Información Federales y el catálogo de controles de seguridad para organizaciones.

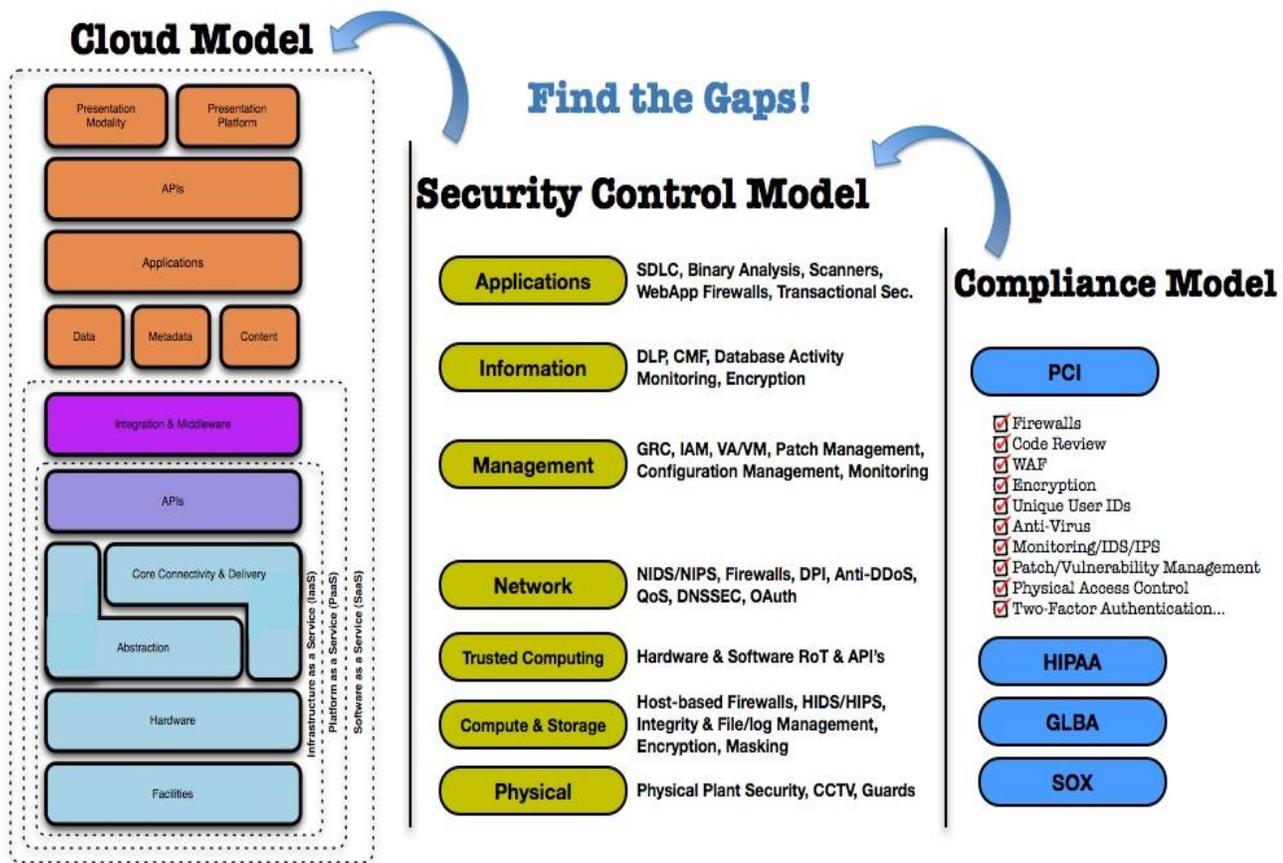


Figura 5— Mapeo del Modelo Cloud para el Control de la Seguridad y el Cumplimiento

1.5.2 ¿Qué es la seguridad para Cloud Computing?

En su mayor parte, los controles de seguridad en *Cloud computing* no son diferentes de los controles de seguridad en cualquier entorno de TI. Sin embargo, debido a los modelos de servicios *Cloud* utilizados, los modelos operativos y las tecnologías que se utilizan para habilitar servicios *Cloud*, *Cloud computing* puede presentar riesgos para una organización diferentes a los de las soluciones de TI tradicionales.

La estrategia en seguridad de una organización se caracteriza por la madurez, la eficacia y la integridad del riesgo ponderado por los controles de seguridad implementados. Estos controles se implementan en uno o más niveles que van desde las instalaciones (seguridad física), a la infraestructura de la red (seguridad de red), a los sistemas TI (seguridad de los sistemas) hasta llegar a la información y a las aplicaciones (seguridad de las aplicaciones). Además, los controles son implementados a nivel humano y de proceso, como es el caso de la segregación de funciones y la gestión de cambios respectivamente.

Como se ha descrito anteriormente en este documento, las responsabilidades en seguridad, tanto del proveedor como del usuario, difieren mucho entre los modelos de servicio *Cloud*. La infraestructura como servicio AWS EC2 de Amazon,

⁷ www.opensecurityarchitecture.org

por ejemplo, incluye la responsabilidad en seguridad del fabricante hasta el hipervisor, lo que significa que sólo pueden abordar controles de seguridad tales como seguridad física, seguridad ambiental y seguridad en la virtualización. El usuario, a su vez, es responsable de los controles de seguridad relativos al sistema TI (instancia) incluyendo el sistema operativo, las aplicaciones y los datos.

Lo contrario es cierto en la oferta SaaS del "customer relationship management" (CRM) de salesforce.com. Debido a que Salesforce.com ofrece toda la "pila", el proveedor no sólo es responsable de los controles de seguridad física y ambiental, sino que también debe abordar los controles de seguridad de la infraestructura, las aplicaciones y los datos. Esto palía mucha de la responsabilidad operativa directa del usuario.

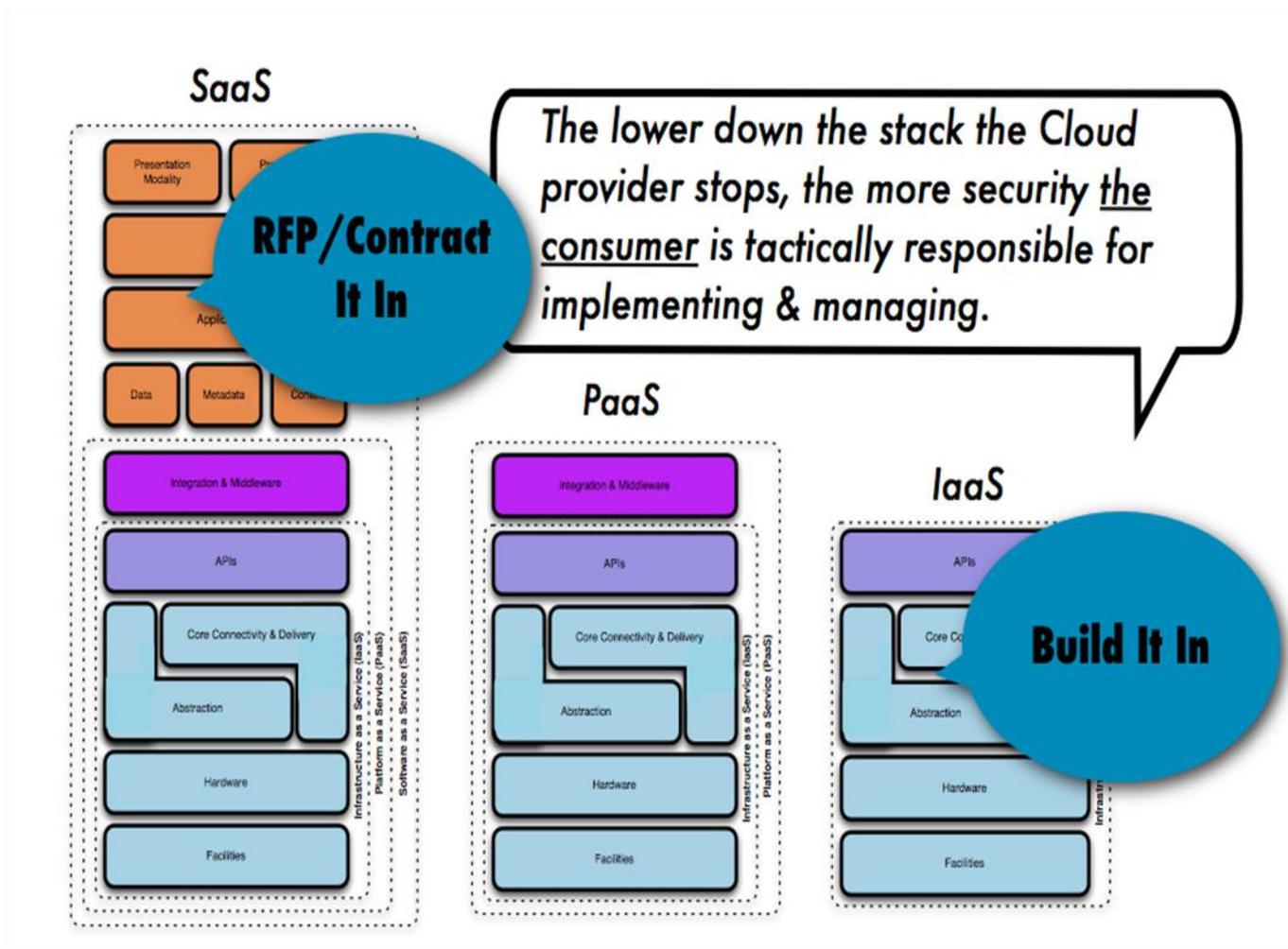


Figura 6—Cómo se integra la seguridad

Actualmente, no existe una manera de que un usuario de servicios *Cloud* inexperto entienda de forma simple de lo que él/ella es exactamente responsable [aunque la lectura de este documento de orientación debería ayudar] pero hay esfuerzos en marcha por parte de CSA y otros organismos para definir los estándares en torno a la auditoría de *Cloud*.

Uno de los atractivos de *Cloud computing* es la eficiencia en costes que ofrecen las economías de escala, la reutilización y la estandarización. Para lograr disponer de estas eficiencias, los proveedores de *Cloud* tiene que proporcionar servicios que sean lo suficientemente flexibles como para servir a la mayor base de clientes posible, maximizando su mercado

objetivo. Por desgracia, la integración de la seguridad en estas soluciones a menudo se percibe como hacerlas más rígidas.

Esta rigidez a menudo se manifiesta en la incapacidad para implementar controles de seguridad en entornos *Cloud* similares a los entornos TI tradicionales. Esto se debe, sobre todo, a la abstracción de la infraestructura y a la falta de visibilidad y capacidad para integrar muchos controles de seguridad habituales, especialmente en la capa de red.

La figura 6 anterior siguiente ilustra estos aspectos: en entornos SaaS los controles de seguridad y su alcance se negocian en los contratos de servicio; los niveles de servicio, la privacidad y el cumplimiento legal son todos temas que se tratarán legalmente en los contratos. En una oferta IaaS, mientras que pertenece al proveedor la responsabilidad de securizar los niveles de infraestructura y abstracción subyacentes, el resto de la pila es responsabilidad del usuario. PaaS ofrece un equilibrio intermedio, donde la responsabilidad de securizar la plataforma recae sobre el proveedor, pero tanto securizar las aplicaciones desarrolladas sobre la plataforma como haberlas desarrollado de forma segura recaen en el usuario.

Comprender el impacto de estas diferencias entre los modelos de servicio y la forma en que se despliegan es vital para la gestión del riesgo en una organización.

1.5.3 Más allá de la Arquitectura: Las Áreas de Enfoque crítico

Los otros trece dominios comprenden el resto de las áreas para valorar de la guía del *Cloud Security Alliance* en materia de *Cloud computing* y están adaptados para abordar los puntos débiles tanto de la seguridad estratégica como táctica dentro de un entorno de *Cloud*, pudiendo ser aplicados a cualquier combinación de servicios *Cloud* y de modelo de despliegue.

Los dominios se dividen en dos grandes categorías: el gobierno *Cloud* y las operaciones. Los dominios de gobierno son amplios y abordan las cuestiones estratégicas y de política dentro de un entorno de *Cloud computing*, mientras que los dominios operacionales se centran en cuestiones más tácticas de la seguridad y de la implementación dentro de la arquitectura.

Tabla 2a— Dominios de gobierno

DOMINIO	LA GUÍA TRATA DE...
Gobierno y Gestión de Riesgos en la Empresa	La capacidad de una organización para controlar y medir el riesgo empresarial introducido por <i>Cloud computing</i> . Aspectos tales como precedentes legales por incumplimiento de acuerdos, capacidad de los usuarios de las organizaciones para evaluar adecuadamente el riesgo de un proveedor de <i>Cloud</i> , responsabilidad de proteger los datos sensibles cuando tanto usuario como proveedor pueden ser responsables y cómo las fronteras internacionales puede afectar a estos temas.
Aspectos legales: Contratos y Descubrimiento Electrónico	Posibles problemas legales cuando se utiliza <i>Cloud computing</i> . Las cuestiones tratadas en esta sección incluyen los requisitos de protección de la información y de los sistemas de computación, las leyes sobre violaciones de

	seguridad por divulgación, los requisitos regulatorios y de privacidad, leyes internacionales, etc.
Cumplimiento Legal y Auditoría	El mantenimiento y la comprobación del cumplimiento legal cuando se utiliza <i>Cloud computing</i> . Cuestiones relativas a la evaluación de cómo <i>Cloud computing</i> afecta al cumplimiento legal con políticas de seguridad internas y también diversos requisitos de cumplimiento (normativos, legislativos y de otro tipo). Este dominio incluye indicaciones para demostrar el cumplimiento legal durante una auditoría.
Gestión de la Seguridad de la Información y de los Datos	La gestión de los datos que son colocados en <i>Cloud</i> . Se discuten aquí aspectos que rodean la identificación y control de datos en <i>Cloud</i> , así como controles de compensación que se pueden utilizar para tratar la pérdida de control físico al mover datos a <i>Cloud</i> . Son mencionados otros puntos, tales como quién es el responsable de la confidencialidad, integridad y disponibilidad.
Portabilidad e Interoperabilidad	La capacidad de mover datos / servicios de un proveedor a otro o traerlos de vuelta por completo a la organización. También trata las cuestiones relacionadas con la interoperabilidad entre proveedores.

Tabla 2b – Dominios Operacionales

DOMAIN	LA GUÍA TRATA DE...
Seguridad Tradicional, Continuidad de Negocio y Recuperación de Desastres	Cómo <i>Cloud computing</i> afecta a los procesos operativos y procedimientos utilizados actualmente para implementar la seguridad, la continuidad de negocio y la recuperación ante desastres. El objetivo es discutir y analizar los posibles riesgos de <i>Cloud computing</i> , con la esperanza de aumentar el diálogo y el debate sobre la abrumadora demanda de mejores modelos de gestión de riesgos empresariales. Además, esta sección trata de ayudar a las personas a identificar dónde los servicios <i>Cloud</i> pueden colaborar para disminuir algunos riesgos de seguridad o pueden acarrear aumentos en otras áreas.
Operaciones de CPD	Cómo evaluar la arquitectura y las operaciones de un proveedor de CPD. Se centra principalmente en ayudar a los usuarios a identificar características comunes de CPDs que podrían ser perjudiciales para la continuidad de los servicios así como características que son fundamentales para la estabilidad a largo plazo.
Respuesta, Notificación y Remediación ante incidentes	La correcta y adecuada detección, respuesta, notificación y remediación ante incidentes. Trata de abordar los elementos que deben estar en su sitio, tanto

	a nivel de proveedor como de usuario, para permitir un manejo de incidentes y un análisis forense adecuados. Este dominio le ayudará a entender las complejidades que los servicios <i>Cloud</i> traen a su programa de gestión de incidentes actual.
Seguridad de las Aplicaciones	Securizar el software de aplicación que se ejecuta en <i>Cloud</i> o está siendo desarrollado en <i>Cloud</i> . Esto incluye aspectos tales como si es apropiado migrar o diseñar una aplicación para que se ejecute en <i>Cloud</i> y, si es este el caso, qué tipo de plataforma es más apropiada (SaaS, PaaS o IaaS).
Cifrado y Gestión de claves	Identificar el uso correcto del cifrado y de una gestión de claves escalable. Esta sección no es prescriptiva, sino que es más bien informativa al discutir por qué es necesario, y determinar cuestiones que se plantean en el uso, tanto para proteger el acceso a los recursos como para proteger los datos.
Gestión de Identidades y de Acceso	La gestión de identidades y el aprovechamiento de los servicios de directorio para proporcionar control de acceso. La atención se centra en los problemas encontrados cuando se extiende la identidad de una organización en <i>Cloud</i> . Esta sección proporciona conocimiento al objeto de evaluar el grado de preparación de una organización para llevar a cabo <i>Identity, Entitlement, and Access Management (IdEA)</i> basado en <i>Cloud</i> .
Virtualización	El uso de la tecnología de virtualización en <i>Cloud</i> . Este dominio aborda temas como los riesgos asociados a <i>multi-tenancy</i> , el aislamiento de Máquinas Virtuales, co-residencia de Máquinas Virtuales, vulnerabilidades del hipervisor, etc. Este dominio se centra en los problemas de seguridad que rodean la virtualización del sistema / hardware en lugar de un estudio más general de todas las formas de virtualización.
Seguridad como Servicio	Servicio por el cual un tercero, proporciona garantía de seguridad, gestión de incidencias, certificación de cumplimiento legal y supervisión de la identidad y del control de acceso. La seguridad como servicio es la delegación de la detección, la corrección y el gobierno de la infraestructura de seguridad a un tercero de confianza con las herramientas y experiencia adecuadas. Los usuarios de este servicio obtienen el beneficio de la experiencia dedicada y la tecnología de vanguardia en la lucha por proteger y bastionar las operaciones comerciales sensibles.

1.6 Modelos de Implementación de *Cloud*

Independientemente del modelo de servicio utilizado (SaaS, PaaS o IaaS) existen cuatro modelos de despliegue de servicios *Cloud* con variaciones derivadas que responden a necesidades específicas.

Es importante tener en cuenta que hay modelos de implementación de *Cloud* derivados y emergentes debido a la maduración de las ofertas del mercado y a la demanda de los clientes. Un ejemplo de este tipo son los servicios *Cloud* privados virtuales - una manera de utilizar la infraestructura de *Cloud* pública de forma privada o semiprivada y de interconectar estos recursos a los recursos internos del CPD de un usuario, generalmente a través de la red privada virtual (VPN).

La mentalidad de arquitectura utilizada en el diseño de "soluciones" tiene claras consecuencias en la futura flexibilidad, seguridad y movilidad de la solución resultante, así como en sus capacidades de colaboración. Como regla general, las soluciones perimetrizadas son menos efectivas que las soluciones des-perimetrizadas en cada una de las cuatro áreas. Por razones similares, se debe dar también una consideración cuidadosa a la elección entre las soluciones propietarias y las soluciones abiertas.

Modelos de implementación

- *Cloud Pública*. La infraestructura *Cloud* está a disposición del público en general o a disposición de un grupo industrial grande y es propiedad de una organización que comercializa servicios *Cloud*.
- *Cloud Privada*. La infraestructura *Cloud* es operada únicamente por una sola organización. Puede ser gestionada por la organización o por un tercero y puede estar ubicada en las instalaciones o fuera de ellas.
- *Cloud Comunitaria*. La infraestructura *Cloud* es compartida por varias organizaciones y da soporte a una comunidad específica que ha compartido preocupaciones (por ejemplo, misión, requisitos de seguridad, política o consideraciones de cumplimiento legal). Puede ser gestionada por las organizaciones o por un tercero, y puede estar ubicada en las instalaciones o fuera de ellas.
- *Cloud Híbrida*. La infraestructura *Cloud* es una composición de dos o más *Clouds* (privada, comunitaria o pública) que siguen siendo entidades únicas pero están unidas por tecnología estandarizada o propietaria que permite la portabilidad de datos y de la aplicación (por ejemplo, proliferación de *Clouds* para balanceo de carga entre *Clouds*).

1.7 Recomendaciones

La entrega de servicios *Cloud* se divide entre tres modelos arquetípicos y diversas combinaciones derivadas. A menudo, a las tres clasificaciones fundamentales se las refiere como el "modelo SPI", donde "SPI" hace referencia al software, a la plataforma o a la infraestructura (como servicio) respectivamente.

- **Cloud Software as a Service (SaaS)**. La capacidad proporcionada al usuario es el uso de las aplicaciones del proveedor que se ejecutan en una infraestructura *Cloud*. Las aplicaciones son accesibles desde diferentes dispositivos cliente a través de una interfaz de cliente ligero como un navegador web (por ejemplo, correo electrónico basado en web). El usuario no gestiona ni controla la infraestructura *Cloud* subyacente que incluye la red, los servidores, los sistemas operativos, el almacenamiento o incluso capacidades de aplicaciones individuales, con la posible excepción de la limitación de parámetros de configuración de aplicaciones específicas de usuario.
- **Cloud Platform as a Service (PaaS)**. La capacidad proporcionada al usuario es el despliegue en la infraestructura *Cloud* de aplicaciones creadas o adquiridas por el usuario con lenguajes y herramientas de programación

soportados por el proveedor. El usuario no gestiona ni controla la infraestructura subyacente que incluye la red, los servidores, los sistemas operativos o el almacenamiento, pero tiene control sobre las aplicaciones desplegadas y posiblemente sobre las configuraciones del entorno de alojamiento de las aplicaciones.

- **Cloud Infrastructure as a Service (IaaS).** La capacidad proporcionada al usuario es la provisión de procesamiento, almacenamiento, interconexión de red y otros recursos de computación fundamentales donde el usuario es capaz de instalar y ejecutar software arbitrario que puede incluir sistemas operativos y aplicaciones. El usuario no gestiona ni controla la infraestructura *Cloud* subyacente, pero tiene el control de los sistemas operativos, el almacenamiento, las aplicaciones desplegadas y, posiblemente, control limitado sobre determinados componentes de red (por ejemplo, firewalls de host).

El modelo del NIST y este documento no abordan directamente las definiciones emergentes del modelo de servicios relacionadas con los intermediarios de servicios *Cloud*. Estos proveedores ofrecen intermediación, monitorización, transformación / portabilidad, gobierno, aprovisionamiento y servicios de integración, y negocian las relaciones entre varios proveedores de *Cloud* y los usuarios.

A corto plazo, debido a que la innovación impulsa rápidos desarrollos de soluciones, los usuarios y los proveedores de servicios *Cloud* podrán disfrutar de diversos métodos de interacción con los servicios *Cloud* en forma de desarrollo de APIs. Por tanto, los intermediarios de servicios *Cloud* surgirán como un importante componente en el ecosistema global *Cloud*.

Los intermediarios de servicios *Cloud* abstraerán estas capacidades e interfaces, posiblemente incompatibles, en beneficio de los usuarios. De esta forma, proporcionarán sustitución antes de la llegada de formas más comunes, abiertas y estandarizadas de resolver el problema a largo plazo con una capacidad semántica que permita al usuario fluidez y agilidad siendo capaces de aprovechar el modelo que mejor se adapte a sus necesidades particulares.

También es importante tener en cuenta la aparición de muchos esfuerzos centrados en el desarrollo tanto de APIs propietarias como abiertas que tratan de habilitar aspectos como la gestión, la seguridad y la interoperabilidad del *Cloud*. Algunos de estos esfuerzos incluyen el *Open Cloud Computing Interface Working Group*, la *Amazon EC2 API*, la *VMware's DMTF-submitted vCloud API*, la *Sun's Open Cloud API*, la *Rackspace API* y la *GoGrid's API*, por nombrar sólo algunos. Las APIs estándar y abiertas jugarán un papel clave en la portabilidad e interoperabilidad de *Cloud* así como en los formatos de contenedores comunes tales como el *DMTF's Open Virtualization Format (OVF)*.

Si bien en este momento hay muchos grupos de trabajo, muchos proyectos y muchas especificaciones publicadas a considerar, es natural que la consolidación se lleve a cabo a medida que las fuerzas de los mercados, la demanda de los consumidores y la economía reduzcan este panorama a un conjunto más manejable e interoperable de actores.

1.8 Requisitos

Los servicios *Cloud* presentan cinco características esenciales que demuestran su relación y sus diferencias con los enfoques tradicionales de computación.

- ✓ **Autoservicio bajo demanda.** Unilateralmente, un usuario puede provisionar capacidades de computación tales como tiempo de servidor y almacenamiento en red de forma automática y según sea necesario, sin necesidad de interacción humana con un proveedor de servicios.

- ✓ **Amplio acceso a la red.** Las capacidades están disponibles en la red y son accedidas a través de mecanismos estándar que promueven el uso de plataformas heterogéneas de clientes ligeros o pesados (por ejemplo, PDA, teléfonos móviles u ordenadores portátiles) así como otros servicios software tradicional o basado en *Cloud*.
- ✓ **Agrupación de recursos.** Los recursos de computación del proveedor son agrupados para dar servicio a múltiples usuarios utilizando un modelo *multi-tenant* con diferentes recursos físicos y virtuales dinámicamente asignados y reasignados de acuerdo con la demanda de usuario. Existe un cierto grado de independencia en la ubicación en el que el cliente generalmente no tiene ningún control o conocimiento sobre la ubicación exacta de los recursos proporcionados, pero puede ser capaz de especificar la ubicación a un nivel más alto de abstracción (por ejemplo, país, estado o CPD). Ejemplos de recursos incluyen el almacenamiento, el procesamiento, la memoria, el ancho de banda y las máquinas virtuales. Incluso las infraestructuras de *Cloud* privadas tienden a agrupar recursos entre las diferentes partes de una misma organización.
- ✓ **Elasticidad rápida.** Las capacidades pueden ser provisionadas rápida y elásticamente - en algunos casos de forma automática - para un escalado rápido hacia fuera y rápidamente liberadas para un escalado hacia dentro. Para el usuario, las capacidades disponibles para la provisión a menudo parecen ser ilimitadas y se pueden comprar en cualquier cantidad y en cualquier momento.
- ✓ **Medición del servicio.** Los sistemas *Cloud* controlan y optimizan automáticamente el uso de recursos mediante el aprovechamiento de una capacidad de medición en un cierto nivel de abstracción adecuado al tipo de servicio (por ejemplo, almacenamiento, procesamiento, ancho de banda o cuentas de usuario activas). El uso de recursos puede ser monitorizado, controlado y reportado, proporcionando transparencia tanto para el proveedor y como para el usuario del servicio.

Las claves para entender cómo la arquitectura *Cloud* impacta la arquitectura de seguridad son un léxico común y conciso emparejado con una taxonomía consistente de ofertas por la cual los servicios y la arquitectura *Cloud* pueden ser desmontados, mapeados a un modelo de seguridad y de controles operacionales compensatorios, a marcos de referencia de evaluación y gestión de riesgos así como a estándares de cumplimiento legal.

Es fundamental comprender cómo cambian o permanecen igual los requisitos de arquitectura, de tecnología, de procesos y de capital humano al desplegar servicios de *Cloud computing*. Sin una comprensión clara de las implicaciones de arquitectura a alto nivel, es imposible abordar asuntos en más detalle de una forma razonable. Esta visión general de la arquitectura, junto con las otras trece áreas críticas, proporcionará al lector una base sólida para evaluar, organizar, gestionar y gobernar la seguridad en entornos de *Cloud computing*.

REFERENCIAS

[1] Definición NIST de *Cloud*. NIST 500-292 “NIST *Cloud Computing* Reference Architecture” (Arquitectura de Referencia del *Cloud Computing* según NIST)

[2] NIST definitions and API homepages (Definiciones NIST y páginas de API) www.cloud-standards.org

[3] Jericho Forum *Cloud* Cube Model (Cubo del Modelo de *Cloud* del Foro Jericho)
www.opengroup.org/jericho/cloud_cube_model_v1.0.pdf



SECCIÓN II //
GOBIERNO EN
ENTORNO *CLOUD*

DOMINIO 2 //

GOBIERNO Y GESTIÓN DEL RIESGO CORPORATIVO

Las cuestiones fundamentales del Gobierno y la Gestión del Riesgo Corporativo en *Cloud computing* tienen que ver con la identificación e implementación de las estructuras organizativas apropiadas junto con los procesos y controles para mantener un gobierno de la información de la seguridad efectivo, manteniendo los aspectos de gestión de riesgo y cumplimiento legal que correspondan. Las organizaciones deben también garantizar una seguridad de la información razonable a lo largo de los flujos de información, incluyendo a sus proveedores, clientes de sus servicios *Cloud* y aquellos socios de negocio con los que trabajen en cualquier modelo de despliegue *Cloud*.

Un programa efectivo de Gobierno y Gestión de Riesgo Corporativo en *Cloud computing* fluye desde los procesos bien desarrollados de Gobierno de la Seguridad de la Información como parte de las obligaciones corporativas en cuanto a debida prudencia. Los procesos de gobierno de la seguridad que estén bien pensados y desarrollados implican programas de seguridad de la información escalables y repetibles a lo largo y ancho de la organización, medibles, con un aspecto de mejora continua y efectivos desde un punto de vista de coste.

Para muchos despliegues *Cloud*, un elemento clave de Gobierno será el acuerdo entre el proveedor y el cliente. Para entornos personalizados, se debe tener un cuidado especial y negociar cada aspecto. Para entornos grandes, tanto para clientes como para proveedores, habrá una decisión de balancear la atención por el detalle con la escalabilidad de dicho esfuerzo. La atención puede ser priorizada en función de la criticidad o el valor en riesgo para esa carga de trabajo específica (por ejemplo, la disponibilidad y tiempo de respuesta pueden ser más importantes para el correo que para un sistema de Recursos Humanos). Con el paso del tiempo, proyectos como *Cloud Audit* o *STAR* proporcionarán modelos de Gobierno más estándar aportando, así, mayor escalabilidad.

Introducción. Este dominio incluye:

- Gobierno
- Gestión de Riesgo Corporativo

Esta sección enlaza con Cloud Control Matrix Controls DG-01, IS-02 y el uso de GRC-XML y CloudAudit para establecer solvencia.

2.1 Gobierno Corporativo

El Gobierno Corporativo es el conjunto de procesos, tecnologías, políticas, leyes e instituciones que afectan a la manera que una compañía está dirigida, administrada o controlada. El Gobierno Corporativo también incluye la relación entre los diferentes actores involucrados y los objetivos de la compañía. El Buen Gobierno está basado en la aceptación de los derechos de las personas interesadas, como verdaderos dueños de la corporación y la responsabilidad de los gestores ejecutivos. Existen muchos modelos de Gobierno Corporativo; sin embargo, todos siguen cinco principios básicos:

- Auditoría de la cadena de suministro
- Estructura del Consejo de Dirección, Gestión Ejecutiva y sus procesos
- Responsabilidad corporativa y cumplimiento Legal
- Transparencia financiera y divulgación de información

- Estructura accionarial y ejercicio de los derechos de control

Un factor fundamental en la decisión de un cliente para contratar o confiar en una corporación es la confianza en que las expectativas se cumplirán. En servicios *Cloud*, las interdependencias entre múltiples servicios hacen que sea más difícil para un cliente conocer quién es la parte responsable, en caso de fallo. Si ello resulta en una falta de confianza en un proveedor en particular, provocará una menor probabilidad de contratación con dicho proveedor. Si esto se convierte en un problema sistémico, la falta de confianza en un actor del mercado puede expandirse a otros y el fallo en el mercado elevaría la posibilidad de acciones externas y la entrada de participantes alternativos.

Las personas interesadas deben considerar con calma los mecanismos de monitorización que son apropiados y necesarios para el crecimiento y rendimiento consistente de la organización.

2.2 Gestión de Riesgo Corporativo

La Gestión de Riesgo Corporativo (ERM, por sus siglas en inglés) está basada en el compromiso de cada organización de proporcionar valor a sus accionistas y personas interesadas. Todos los negocios se enfrentan a incertidumbres y uno de los retos de la gestión empresarial es determinar cómo una organización puede medir, gestionar y mitigar las mismas. La incertidumbre representa al mismo tiempo una oportunidad y un riesgo con un potencial de aumentar o reducir el valor de la organización y sus estrategias.

La gestión del riesgo de la información es el proceso de identificar y comprender la exposición al riesgo junto con la capacidad de gestionarlo, alineado con la tolerancia al riesgo por parte del dueño de los datos. En consecuencia, es el primer criterio de decisión para los recursos de tecnología dedicados a proporcionar confidencialidad, integridad y disponibilidad de los activos de la información.

La gestión de riesgo empresarial en los negocios incluye los métodos y procesos usados por las organizaciones para gestionar riesgos y abordar oportunidades relacionadas con la consecución de sus objetivos. En un entorno *Cloud*, la dirección ejecutiva selecciona una estrategia de respuesta frente a riesgos específicos identificados y analizados, que pueden incluir:

- Evitar el riesgo—cesando las actividades que elevan el riesgo
- Reducir el riesgo—realizando acciones que reduzcan la probabilidad o el impacto relacionado con el riesgo
- Compartir el riesgo—transfiriendo o contratando un seguro que pueda financiar el potencial impacto
- Aceptar el riesgo—no se toma ninguna acción debido al análisis coste/beneficio

Esta sección enlaza con Cloud Control Matrix Controls DG-08 y el uso de ISO31000, ISF y las guías de ISACA para establecer solvencia.

La gestión de riesgo es, por naturaleza, un proceso equilibrado no necesariamente con el objetivo de reducir la incertidumbre sino con la meta de maximizar el valor en sintonía con la tolerancia al riesgo de la entidad y su estrategia.

Existen muchas variables, valores y riesgos en cualquier oportunidad en *Cloud* que afectan a la decisión de si un servicio *Cloud* debe ser adoptado desde un punto de vista de riesgo o de valor para el negocio. Cada organización debe considerar esas variables para decidir si *Cloud* es una solución apropiada para sus objetivos.

Cloud computing ofrece a las compañías muchos beneficios posibles; algunos de ellos son:

- Utilización optimizada de recursos
- Ahorro de costes
- Transformación de los costes de inversión (CAPEX) a costes de operación (OPEX)
- Escalabilidad dinámica (elasticidad) de los activos de tecnología
- Reducción del ciclo de vida del desarrollo
- Tiempos más cortos para la implantación de nuevas iniciativas

Los clientes deben ver la seguridad en *Cloud* entendiendo los problemas de seguridad que pueden afectar su cadena de suministro. Esto implica examinar la cadena de suministro del proveedor (sus relaciones y dependencias) hasta donde sea posible; requiriendo, a su vez, revisar la gestión que el proveedor hace de sus socios y proveedores. El conocimiento de los que abastecen al proveedor debe incluir su gestión de incidencias, la continuidad del negocio, las políticas de recuperación frente a desastres y sus procesos y procedimientos; debe, asimismo, incluir una revisión de dónde está físicamente alojada la información y las dependencias de respaldo. Debe incluir también una revisión de cómo el proveedor garantiza su compromiso con sus propias políticas y procedimientos y las métricas que proporcionen información razonable respecto del rendimiento y eficacia de los controles implantados. La información de incidentes puede ser especificada en contratos, acuerdos de niveles de servicio u otros acuerdos y debe ser comunicada automática o periódicamente, integrada en los sistemas de gestión de avisos e información o entregada a personal relevante. El nivel de atención y detalle debe estar alineado con el valor que está en riesgo -si la compañía contratada no accede directamente a los datos empresariales, entonces el nivel de riesgo se reduce significativamente y viceversa -.

Los clientes deben revisar los procesos de gestión de riesgo y gobierno de sus proveedores y garantizar que las prácticas son consistentes y están alineadas.

2.3 Permisos

- Adoptar un marco de referencia de gestión del riesgo para la monitorización y medición de riesgo corporativo.
- Adoptar métricas alrededor del rendimiento de la gestión del riesgo (por ejemplo, Security Content Automation Protocol (**SCAP**⁸, Cybersecurity Information Exchange Framework (**CYBEX**)⁹, o **GRC-XML**¹⁰).
- Adoptar una visión centrada en el riesgo para el Gobierno Corporativo, de tal forma que la dirección ejecutiva tome un papel de confianza tanto para los accionistas como para las personas interesadas en la cadena de suministro.
- Adoptar un marco de referencia desde la perspectiva legal de manera que se consideren las diferencias entre áreas geográficas.

⁸ **SCAP** - Security Content Automation Protocol

⁹ **CYBEX** - Cybersecurity Information Exchange Framework

¹⁰ **GRC-XML** - estándar de tecnología que permite y mejora la transferencia de información entre varias tecnologías que apoyan iniciativas GRC

2.4 Recomendaciones

- Reinvertir los ahorros de costes obtenidos en *Cloud* en mejorar el escrutinio de las capacidades de seguridad del proveedor, la aplicación de las medidas de seguridad, las evaluaciones detalladas y auditorías que garanticen que los requisitos se cumplen de manera continua.
- Las compañías cliente deben incluir la revisión específica de sus procesos y estructura del gobierno de la seguridad de la información, así como de los controles específicos de seguridad como parte de su debida diligencia en relación a futuras organizaciones proveedoras de servicios. Los procesos de seguridad y gobierno de los proveedores y sus capacidades deben ser revisadas en términos de suficiencia, madurez y consistencia con los procesos de gestión de la seguridad de la información del usuario. Los controles de seguridad de la información del proveedor deben estar basados en la función del riesgo y apoyar claramente los procesos de gestión.
- Se deben identificar estructuras y procesos colaborativos de gobierno entre clientes y proveedores cuando sea necesario, tanto por la parte de diseño y desarrollo del servicio como por lo que respecta a la entrega del mismo, debe realizarse como un servicio de gestión del riesgo, que debe ser incorporado en los acuerdos de niveles de servicio.
- Los departamentos de seguridad deben participar en las conversaciones en las que se establezcan acuerdos de niveles de servicio (**ANS**) y obligaciones contractuales para garantizar que los requisitos de seguridad son direccionados desde un punto de vista de contrato.
- Deberán ser establecidos métricas y estándares para la medición del rendimiento y la efectividad de la gestión de la seguridad de la información antes de llevar la organización a *Cloud*. Como mínimo, las organizaciones deberán entender y documentar sus métricas actuales y cómo éstas cambiarán cuando las operaciones se trasladen a *Cloud* donde, potencialmente, un proveedor puede utilizar diferentes indicadores.
- Debido a la falta de control físico por parte de los clientes sobre la infraestructura, en muchos despliegues de *Cloud*, los acuerdos de niveles de servicio que se indiquen en el contrato, los requisitos legales y la documentación del proveedor, juegan un papel mucho mayor en la gestión del riesgo si lo comparamos con lo tradicional donde las empresas han sido propietarias de su propia infraestructura.
- Debido a los aspectos de múltiples instancias y aprovisionamiento bajo demanda de *Cloud*, las aproximaciones tradicionales de auditoría y asesoramiento pueden no resultar útiles, no estar disponibles o pueden ser modificadas. Por ejemplo, algunos proveedores restringen los estudios de vulnerabilidades y los test de ataques de intrusión, mientras otros limitan la disponibilidad de los logs de auditoría y las actividades de monitorización. Si estos son requeridos por la política interna del cliente, puede ser necesario buscar alternativas, indicar excepciones contractuales específicas o un proveedor alternativo mejor alineado con las exigencias de la gestión de riesgo de la compañía.
- Si los servicios proporcionados en *Cloud* son esenciales para las operaciones empresariales, el ejercicio de gestión de riesgos debe identificar y valorar correctamente los activos, identificar y analizar las amenazas y vulnerabilidades y su potencial impacto (escenarios de riesgo e incidentes), analizar la probabilidad de que ocurran eventos, disponer de un nivel de riesgo aceptado por la dirección junto con el desarrollo de planes de

tratamiento con múltiples opciones (controlar, evitar, transferir, aceptar). Los resultados de los planes de tratamiento de riesgos deben ser incorporados en los niveles de servicio que se vayan a acordar.

- Las aproximaciones de gestión de riesgos entre el proveedor y el usuario deben ser consistentes con los criterios de análisis de impacto y la definición de probabilidad. El usuario y el proveedor deben, de común acuerdo, desarrollar escenarios de riesgos para el servicio *Cloud*; esto debe ser intrínseco en el diseño del servicio del proveedor y en el asesoramiento de riesgos de uso del servicio por parte del usuario.
- Debido a la cambiante naturaleza de *Cloud* y sus proveedores, debe tenerse en cuenta el riesgo asociado al proveedor; por ejemplo, la capacidad de supervivencia, la portabilidad de los datos y aplicaciones y la interoperabilidad de los servicios.
- Los inventarios de activos deben incluir aquellos que estén involucrados en servicios en *Cloud* y bajo el control del proveedor. La clasificación de activos y esquemas de valoración deben ser consistentes entre el usuario y el proveedor.
- El servicio, y no solo el proveedor o fabricante, debe ser objeto de un análisis de riesgos. El uso de servicios en *Cloud*, y en particular el/los servicio/s y los modelos de despliegue utilizados, deben ser consistentes con los objetivos de gestión de riesgos de la organización así como con sus objetivos de negocio.
- Los clientes y los proveedores de servicio de *Cloud* deben desarrollar un Gobierno de la seguridad de la información robusto, independientemente del modelo de despliegue o de servicio. El Gobierno de la seguridad de la información debe ser colaborativo entre clientes y proveedores para conseguir los objetivos establecidos de antemano que den soporte a la misión del negocio y al programa de seguridad de la información. La función de Gobierno debe incluir revisiones periódicas y el modelo de servicio puede ajustar los roles y responsabilidades definidas (basado en el correspondiente alcance de control para el usuario y el proveedor), mientras que el modelo de despliegue puede definir responsabilidades y expectativas (basadas en la gestión de riesgo).
- Los clientes de servicios *Cloud* deben preguntarse si su dirección ejecutiva ha definido la tolerancia al riesgo con respecto a esos servicios y si ha aceptado cualquier riesgo residual de la utilización de los mismos.
- Cuando un proveedor no pueda demostrar que tiene procesos coherentes y efectivos de gestión de riesgos en relación a sus servicios, los clientes deberán evaluar cuidadosamente la utilización de ese proveedor así como la capacidad de la organización cliente de compensar las deficiencias potenciales en dicha gestión de riesgos.
- En el modelo de relación con los proveedores, las organizaciones deben definir métricas de riesgo que estén basados en factores de exposición tanto de negocio como técnicos. Estas métricas pueden incluir el tipo de dato al que se refieren, la variedad de tipos de clientes relacionados con esa información y también los proveedores u otras organizaciones implicadas en su tratamiento.

2.5 Requisitos

- ✓ Proporcionar transparencia a las personas interesadas y accionistas demostrando solvencia fiscal y transparencia organizativa.

- ✓ Respetar la interdependencia de los riesgos inherentes en la cadena de suministro *Cloud* y comunicar la postura corporativa frente al riesgo así como su disposición para clientes y partes implicadas.
- ✓ Inspeccionar y tener en cuenta los riesgos heredados de otros miembros de la cadena de suministro y realizar acciones proactivas para mitigar y contener los riesgos a través de la capacidad de supervivencia de la organización.

DOMINIO 3 //

CUESTIONES LEGALES: CONTRATOS Y eDISCOVERY

El presente capítulo destaca algunas de las cuestiones legales que suscita *Cloud* computing. Trata de facilitar un marco general de aspectos legales que pueden surgir al trasladar datos a *Cloud*, algunos aspectos dignos de consideración en los contratos de prestación de servicios *Cloud* y las problemáticas específicas que se derivan del eDiscovery en la legislación occidental.

Los aspectos abordados en este capítulo se tratan de forma general, y no deben considerarse como sustitutos de la obtención de asesoramiento jurídico.

Introducción. Este capítulo trata los siguientes temas:

- Resumen de las principales cuestiones legales derivadas del traslado de datos a *Cloud*
- Aspectos dignos de consideración en los contratos de prestación de servicios de *Cloud*
- Problemáticas específicas derivadas del eDiscovery.

3.1 Cuestiones legales

Son muchos los países, a lo largo del globo, en los que existen leyes, reglamentos y otras normas que exigen la protección de la privacidad de los datos personales y la seguridad de la información en los sistemas informáticos, tanto a organizaciones públicas como privadas. Por ejemplo, en la región Asia-Pacífico, Japón, Australia, Nueva Zelanda y muchos otros países han aprobado leyes de protección de datos, que obligan al responsable del tratamiento a adoptar aquellas medidas técnicas, físicas y administrativas que resulten razonables para la protección de los datos personales ante pérdidas, usos o alteraciones no autorizadas, partiendo de las Directrices de Privacidad y Seguridad de la Organización para la Cooperación y el Desarrollo Económico (OCDE)¹¹ y del Marco de Privacidad del foro de Cooperación Económica Asia-Pacífico (APEC).¹²

En Europa, los Estados miembros del Espacio Económico Europeo (EEE)¹³ han aprobado sus leyes de protección de datos siguiendo los principios establecidos en las Directivas de la Unión Europea de Protección de Datos, de 1995,¹⁴ y de Privacidad y Comunicaciones Electrónicas (ePrivacy), de 2002 (modificada en 2009). Estas normas incluyen un componente de seguridad, según el cual la obligación de suministrar un seguridad adecuada debe trasladarse a los subcontratistas. Otros países que mantienen lazos estrechos con el EEE, como Marruecos y Túnez en África, o Israel y Dubai en Oriente Medio, han adoptado igualmente leyes similares que siguen los mismos principios.

Los países de América del Norte, Central y del Sur están adoptando, igualmente, leyes de protección de datos a un ritmo rápido. Todas estas leyes incluyen requisitos de seguridad, y sitúan la carga de asegurar la protección y seguridad de los datos personales en su custodio, con independencia del lugar en el que se encuentren situados y, en especial, si son

¹¹ En inglés, "Organization for Economic Cooperation and Development" (OECD)

¹² Acrónimo del inglés "Asia Pacific Economic Cooperation" (APEC)

¹³ En inglés, European Economic Area (EEA)

¹⁴ Directiva 95/46/CE

transferidos a terceros. Por ejemplo, además de las leyes de protección de datos de Canadá, Argentina y Colombia, que llevan vigentes algunos años, México, Uruguay y Perú han aprobado recientemente leyes de protección de datos que se inspiran principalmente en el modelo Europeo, pero que también pueden incluir referencias al Marco de Privacidad de APEC.

En Japón, la Ley de Protección de la Información Personal exige al sector privado que proteja la información personal y los datos de forma segura. En el sector sanitario, existen normas sectoriales como la Ley de Médicos, la Ley de Enfermeras de Salud Pública, Matronas y Enfermeras, y la Ley de Farmacéuticos, que exigen confidencialidad a los profesionales registrados de la salud con respecto a los datos de sus pacientes. Igualmente, las organizaciones que hagan negocios en Estados Unidos pueden estar sometidas a una o más leyes de protección de datos. Las leyes hacen a dichas organizaciones responsables por las actuaciones de sus subcontratistas. Por ejemplo, las reglas de seguridad y privacidad de la Ley Gramm-Leach-Bliley¹⁵ o de la Ley de Portabilidad y Responsabilidad en los Seguros de Salud, de 1996 (HIPAA), exigen que las organizaciones obliguen a sus subcontratistas, a través de contratos escritos, a implementar medidas razonables de seguridad y a cumplir con la normativa de privacidad de datos. Agencias gubernamentales, como la Comisión Federal de Comercio (FTC) o las Fiscalías Generales de los Estados han reconocido, en consecuencia, la responsabilidad de las organizaciones por las actividades de sus subcontratistas. Los Estándares de Seguridad de Datos (Data Security Standards, DSS) de la Payment Card Industry (PCI), que se aplican a los datos de las tarjetas de crédito en todo el mundo, incluyendo los datos tratados por subcontratistas, establecen requerimientos similares.

Los apartados siguientes muestran ejemplos de cuestiones legales que pueden surgir en relación con la transferencia de datos personales a *Cloud* o el tratamiento de datos personales en ella.

Tabla 3 — Implicaciones obligatorias

CUESTIÓN	DESCRIPCIÓN
Leyes Federales de los Estados Unidos	Numerosas leyes federales y sus correspondientes reglamentos, como la GLBA, la HIPAA, la COPPA (Ley de Protección de la Privacidad de los Menores en Internet, de 1998), así como las resoluciones de la FTC, exigiendo a las empresas la adopción de medidas específicas de privacidad y seguridad al tratar datos, requiriendo precauciones similares en sus contratos con terceros prestadores de servicios.
Leyes Estatales de los Estados Unidos	Numerosas leyes estatales establecen, igualmente, obligaciones sobre las empresas, para implementar medidas de seguridad adecuadas sobre los datos personales, y para exigir a sus prestadores de servicios que hagan lo mismo. Las leyes estatales que regulan aspectos de la seguridad de la información requieren, como mínimo, que la empresa celebre un contrato por escrito con el prestador de servicios, que incluya unas medidas de seguridad razonables. Véase, por ejemplo, los amplios requisitos fijados por los Reglamentos de Seguridad de Massachusetts.
Estándares	Estándares como PCI DSS o ISO 27001 crean también un efecto dominó, similar al de las leyes federales y estatales. Las empresas sometidas a PCI DSS o ISO 27001 deben respetar unos estándares concretos y trasladar a sus subcontratistas las mismas obligaciones, si quieren cumplir con el estándar al que se han sometido.
Normativas Internacionales	Muchos países cuentan con normas de protección de datos que siguen el modelo de la Unión Europea, el de la OCDE o el de APEC. De acuerdo con dichas leyes, el responsable del tratamiento (básicamente, la entidad que establece la relación inicial con la persona) conserva la responsabilidad por el recabado y el tratamiento de los datos personales, incluso cuando son tratados por terceros. El responsable del tratamiento está obligado a asegurar que cualquier tercero que trate datos en su nombre implemente las medidas de seguridad técnicas y organizativas adecuadas para proteger los datos.
Obligaciones contractuales	Incluso en casos en que una actividad concreta no está regulada, las empresas pueden estar sometidas a obligaciones contractuales para proteger la información de sus clientes, contactos o empleados; asegurar

¹⁵ En inglés, **GLBA** - Gramm-Leach-Billey Act

	<p>que los datos no se utilizan para fines secundarios; y que no son cedidos a terceros. Esta obligación puede derivarse, por ejemplo, de los Términos y Condiciones y de la Declaración de Privacidad que una empresa publica en su sitio web.</p> <p>De forma alternativa, la empresa puede haber celebrado contratos (como acuerdos de prestación de servicios) con sus clientes, en los que haya asumido compromisos específicos para proteger los datos (personales o empresariales), limitando su uso, asegurando su seguridad, cifrándolos, etc.</p> <p>Las organizaciones deben asegurarse de que, cuando los datos que custodien sean hospedados en <i>Cloud</i>, siguen siendo capaces de cumplir las promesas y compromisos asumidos en sus avisos de privacidad o en otros contratos.</p> <p>Por ejemplo, la empresa puede haberse comprometido a tratar los datos únicamente para determinados usos. Los datos en <i>Cloud</i> deben ser utilizados sólo para las finalidades para las que fueron recabados.</p> <p>Si el aviso de privacidad permite a las personas afectadas acceder a sus datos personales, y a modificar o cancelar dicha información, el prestador de servicios <i>Cloud</i> debe permitir igualmente el ejercicio de los derechos de acceso, modificación y cancelación, de forma idéntica a la que se daría en una relación en la que no se emplease <i>Cloud</i>.</p>
<p>Prohibición de las transferencias internacionales</p>	<p>Muchas leyes, alrededor del globo, prohíben o limitan la transferencia de información fuera del país. En la mayoría de los casos, la transferencia se permite únicamente si el país receptor de los datos ofrece una protección adecuada de la información personal y de los derechos de privacidad. La finalidad de este requisito de adecuación es asegurar que las personas afectadas cuyos datos se transfieran a otros países sean capaces de disfrutar, en el país receptor, de unos derechos y protecciones en materia de privacidad similares, y no inferiores, a los garantizados antes de la transferencia.</p> <p>Por tanto, es importante para un usuario de <i>Cloud</i> conocer la localización de los datos personales de sus empleados, clientes... de manera que pueda identificar las restricciones que le puedan imponer las leyes de privacidad de otros países.</p> <p>Dependiendo del país, los requisitos para asegurar este nivel de protección adecuado pueden ser complejos y rigurosos. En algunos casos, puede ser preciso obtener la autorización previa de la Autoridad de Protección de Datos local.</p>

3.2 Consideraciones contractuales

Cuando los datos son transferidos a *Cloud*, la responsabilidad de su protección y seguridad sigue siendo, habitualmente, de quien los recaba o custodia, si bien bajo algunas circunstancias esta responsabilidad puede estar compartida con otros. Cuando se encarga a un tercero que aloje o trate estos datos, el custodio de los datos sigue respondiendo ante cualquier pérdida, daño o uso no autorizado de los datos. Es prudente, y en ocasiones obligatorio, que el custodio y el prestador de servicios de *Cloud* firmen un contrato por escrito que defina claramente las funciones y expectativas de las partes, y las responsabilidades que corresponden a cada una de ellas en relación con los datos en cuestión.

Las leyes, reglamentos, estándares y las buenas prácticas relacionadas que se abordaron con anterioridad, exigen igualmente a los custodios que aseguren que dichas obligaciones se cumplen, realizando *due diligence* (antes de la ejecución del contrato) o auditorías de seguridad (durante la ejecución del contrato).

3.2.1 Due Diligence

Antes de celebrar un acuerdo de *Cloud computing*, la empresa debe analizar sus propias prácticas, necesidades e impedimentos, en aras a identificar las barreras legales y los requisitos a cumplir, en relación con la transacción de *Cloud computing* propuesta. Por ejemplo, debe determinar si su modelo de negocio permite el uso de servicios de *Cloud computing* y bajo qué condiciones. La naturaleza de su negocio puede implicar que cualquier cesión del control de los datos de la empresa esté prohibida por ley o cree graves problemas de seguridad.

Además, la empresa debe, y en algunos casos puede estar obligada por ley, llevar a cabo una *due diligence* sobre el prestador de servicios de *Cloud* propuesto, en aras a determinar si la oferta permitirá a la empresa cumplir con su obligación de proteger sus activos de forma continuada.

3.2.2 Contrato

Las partes deben celebrar un contrato por escrito. Dependiendo de la naturaleza de los servicios, puede ser habitual que el contrato se acepte haciendo clic en un acuerdo de adhesión, en el que no cabe negociación; o que las partes negocien un documento por escrito más complejo, adaptado a la situación específica. Si el acuerdo de adhesión es el único acuerdo disponible, el cliente del servicio *Cloud* debe considerar los riesgos de unas posteriores negociaciones, frente a los beneficios reales, los ahorros económicos y la facilidad de uso prometida por el prestador del servicio *Cloud*. Si las partes pueden negociar un contrato, deben asegurarse de que las cláusulas de dicho contrato aborden las necesidades y obligaciones de las partes, tanto durante la duración del contrato como con posterioridad a su finalización. Deben negociarse unas cláusulas detalladas y exhaustivas, que aborden las necesidades y riesgos específicos de utilizar un entorno *Cloud*.

Si existen problemas no previstos en el contrato, el cliente del servicio *Cloud* debe considerar métodos alternativos de alcanzar sus objetivos, un proveedor alternativo o no colgar sus datos en *Cloud*. Por ejemplo, si el cliente del servicio *Cloud* desea colgar información afectada por HIPAA en *Cloud*, el cliente necesitará encontrar un prestador de servicios que firme con él un acuerdo de negocio asociado, conforme a la HIPAA, o no pasar, en caso contrario, sus datos a *Cloud*.

A continuación se incluyen descripciones breves de algunas problemáticas específicas del *Cloud*. Además, se adjunta una lista de control completa (pero no exhaustiva) que recoge las cuestiones a tener en cuenta al revisar un contrato de servicios *Cloud*.

3.2.3 Supervisión, realización de pruebas y actualización

El entorno de *Cloud* no es estático. Evoluciona, y las partes deben adaptarse. Se recomiendan realizar tareas de supervisión periódica, prueba y análisis de servicios, a efectos de asegurar que las medidas de privacidad y seguridad exigidas se están utilizando, y que los procesos y políticas se están cumpliendo. Además, el panorama legal, regulatorio y técnico puede cambiar a un ritmo rápido. Nuevas amenazas de seguridad, nuevas leyes, nuevos requisitos de cumplimiento que deben ser abordados con prontitud. Las partes deben mantenerse al día en relación con los requisitos legales y de otro tipo, para asegurar que las operaciones siguen siendo lícitas; y en relación con las medidas de seguridad implementadas, para que vayan evolucionando según surgen nuevas tecnologías y leyes.

CloudAudit y Cloud Trust Protocol son dos mecanismos que automatizan la supervisión y la realización de pruebas en las cadenas de producción *Cloud*. Además, UIT-T está trabajando en una especificación de Auditoría de Cloud X.1500, denominada CYBEX.

3.3 Problemáticas específicas derivadas del E-Discovery

Este apartado aborda los requisitos específicos de litigación en los Estados Unidos. Los litigantes en EE.UU. fundamentan gran parte de sus argumentos de defensa en documentos. Una de las peculiaridades del sistema judicial estadounidense, en claro contraste con la mayoría de países, es que un litigante debe facilitar a su contrario TODOS los

documentos relacionados con el caso. No puede limitarse a aportar los documentos que le resulten favorables, sino también los que resultan favorables para su contraparte.

En los últimos años, se han producido numerosos escándalos en los que los litigantes fueron acusados de haber borrado, perdido o modificado, de forma voluntaria, pruebas que les perjudicaban en sus casos. A raíz de ello, las normas procesales fueron modificadas para clarificar las obligaciones de las partes, en especial en el caso de información almacenada electrónicamente (por sus siglas en inglés, “ESI”).

Desde que *Cloud computing* se está convirtiendo en el repositorio de la mayor parte de la ESI que se precisa en una causa o investigación, los prestadores de servicios *Cloud* y sus clientes deben planificar cuidadosamente cómo poder identificar todos los documentos pertenecientes a un caso, en aras a poder cumplir con los estrictos requisitos impuestos por las normas de eDiscovery de las Reglas Federales de Procedimiento Civil, y de los equivalentes estatales a dichas leyes.

En este sentido, el cliente de un servicio *Cloud* y el proveedor han de tener en cuenta las siguientes cuestiones en asuntos en los que el cliente esté sometido a peticiones de Discovery, y el prestador de servicios *Cloud* cuente con datos potencialmente relevantes.

3.3.1 Posesión, custodia y control

En la mayor parte de las jurisdicciones de los Estados Unidos, la obligación que tiene cada parte de producir información relevante se limita a los documentos y datos que se encuentren bajo su posesión, custodia o control. Alojar datos relevantes en un tercero, incluso en un prestador *Cloud*, no exime a dicha parte de la obligación de producir información en la medida en que tenga un derecho legal de acceder y obtener los datos. Sin embargo, puede que no todos los datos alojados por un prestador *Cloud* estén bajo el control del cliente (por ejemplo, planes de recuperación ante desastres, ciertos metadatos creados y mantenidos por el prestador de servicios *Cloud* para operar su entorno). Distinguir entre los datos que están y que no están a disposición del cliente puede ser interesante tanto para el prestador como para el propio cliente. Las obligaciones del prestador de servicios *Cloud*, como encargado de manejar los datos, en relación a la producción de información en respuesta al proceso legal, es un asunto que debe resolver cada jurisdicción.

3.3.2 Entornos y aplicaciones de *Cloud* relevantes

En ciertas causas e investigaciones, la propia aplicación o entorno *Cloud* pueden, en sí mismos, ser relevantes para resolver la controversia en la causa o investigación. En tales circunstancias, la aplicación y el entorno podrían quedar fuera del control del cliente, por lo que se necesitaría una citación u otro proceso de Discovery dirigido directamente al prestador.

3.3.3 Capacidad de búsqueda y herramientas de eDiscovery

Dadas las peculiaridades del entorno *Cloud*, un cliente quizás no puede aplicar o utilizar en él las mismas herramientas de eDiscovery que utiliza en sus propios entornos. Es más, puede que el cliente carezca de la posibilidad o de los privilegios administrativos para buscar o acceder a todos los datos alojados en *Cloud*. Por ejemplo, mientras que el cliente puede acceder a multitud de cuentas de correo electrónico de sus empleados desde su propio servidor en una

sola vez, quizás no podría hacerlo si las cuentas de correo electrónico estuviesen alojadas en *Cloud*. Por ello, los clientes necesitan contabilizar el tiempo y gastos potenciales adicionales que tal limitación les pudiese causar.

3.3.4 Conservación

En términos generales, en los Estados Unidos cada parte está obligada a adoptar medidas razonables para impedir la destrucción o modificación de los datos que posee, custodia o controla, que sepa o deba razonablemente saber que son relevantes para una causa o investigación pendiente o que se pueda predecir razonablemente. Dependiendo del servicio *Cloud* y del modelo de despliegue que el cliente utilice, la conservación en *Cloud* puede ser muy similar a la conservación en otras infraestructuras de TI, o ser mucho más compleja.

En la Unión Europea, la conservación de la información está regulada por la Directiva 2006/24/CE, del Parlamento Europeo y del Consejo, de 15 de marzo de 2006. Japón, Corea del Sur y Singapur cuentan con iniciativas de protección de datos similares. En América del Sur, Brasil y Argentina tienen la Ley Azeredo y la Ley de Conservación de Datos de Argentina de 2004, nº 25.873, de 6 de febrero de 2004, respectivamente.

3.3.4.1 Costes y almacenamiento

La conservación puede implicar que grandes cantidades de información se mantengan durante largos períodos. ¿Cuáles son las consecuencias de esto bajo un Acuerdo de Nivel de Servicio (“ANS”)? ¿Qué ocurre si los requisitos de conservación van más allá de los plazos del ANS? Si el cliente conserva los datos allí, ¿quién paga por la ampliación del almacenamiento y a qué coste? ¿Está cubierto el cliente por el ANS, en lo relativo a la capacidad de almacenamiento? ¿Puede el cliente descargar datos de forma eficaz, y sólida desde un punto de vista forense, para conservarlos offline o casi en línea?

3.3.4.2 Ámbito de conservación

A falta de una causa justificada o de una necesidad específica, el solicitante está legitimado únicamente para acceder a aquellos datos alojados en *Cloud* que contengan información relevante, y no a todos los datos que se encuentren en *Cloud* o en la aplicación. Sin embargo, si el cliente no es capaz de conservar la información relevante o los datos de forma desagregada, podría verse obligado a conservar una información excesiva, en aras a efectuar la conservación razonable, en función de la causa o investigación.

3.3.4.3 Almacenamiento dinámico y compartido

La carga de la conservación de datos en *Cloud* puede ser relativamente pequeña si el cliente tiene espacio para mantenerlos en dicho lugar, si los datos son relativamente estáticos o si la no accede mucha gente y sabe cómo conservarlos. Sin embargo, en un entorno *Cloud* que modifica o elimina datos de forma programada, o en el que los datos se comparten con gente que no es consciente de la necesidad de conservarlos, su conservación puede ser más complicada. Una vez que el cliente determina que dichos datos son relevantes y deben ser conservados, el cliente podría tener que trabajar con el prestador para definir un modo razonable para conservar dichos datos.

3.3.5 Recabado

Dada la potencial falta de permisos administrativos que un cliente tiene sobre los datos en *Cloud*, el recabado de datos desde *Cloud* puede ser más complicado, llevar más tiempo y ser más caro que si se hiciese en los sistemas del cliente. En

concreto, un cliente puede no gozar del mismo nivel de visibilidad sobre sus datos en *Cloud*, y tener más dificultades para comparar los datos que ha recabado con los datos en *Cloud*, para determinar que la exportación se ha realizado de forma razonablemente completa y precisa.

3.3.5.1 Acceso y ancho de banda

En la mayor parte de los casos, el acceso de los clientes a sus datos en *Cloud* vendrá determinado por su ANS. Esto puede limitar su capacidad de recabar grandes cantidades de datos de forma rápida y sólida desde un punto de vista forense (por ejemplo, preservando todos los metadatos que resulten razonablemente relevantes). Los clientes y los prestadores *Cloud* harían bien en tener en cuenta esta cuestión con anticipación, y en establecer un protocolo (y un coste) para accesos extraordinarios para recabar información en caso de causas judiciales e investigaciones. A falta de tales acuerdos, los clientes deben tener en cuenta el tiempo y costes adicionales que implicaría el recabado en *Cloud* al plantear alegaciones frente a los solicitantes de información y los tribunales.

3.3.5.2 Funcionalidades

Se trata de una cuestión relacionada con el acceso y ancho de banda, pero diferente a ellos. Los privilegios de acceso de los clientes pueden permitirles acceder al rango completo de datos, pero no el grado de funcionalidades más adecuado en una situación determinada. Por ejemplo, el cliente podría tener acceso a tres años de datos de transacciones concretas, pero ser únicamente capaz de descargar los datos correspondiente a dos semanas de cada vez, por limitaciones funcionales. Igualmente, un cliente podría no poder visualizar todos los metadatos existentes en realidad, sino únicamente un número limitado de metadatos.

3.3.5.3 Técnicas forenses

Realizar una imagen bit a bit desde una fuente de datos en *Cloud* es generalmente difícil o imposible. Por motivos obvios de seguridad, los prestadores son reticentes a permitir el acceso a su hardware, particularmente en un entorno multitenant, donde los clientes podrían lograr acceder a los datos de otros clientes. Incluso en *Cloud* privadas, aplicar técnicas forenses puede ser extremadamente complicado, y los clientes pueden tener que comunicar al abogado de la parte contraria o a los tribunales estas limitaciones. Afortunadamente, no es habitual que se ordenen técnicas forenses en *Cloud*: no por ser *Cloud*, sino porque está estructurado a través de una jerarquía de datos o virtualización que no permite, por sí misma, los análisis forenses.

3.3.5.4 Integridad razonable

Un cliente sometido a una petición de Discovery debe tomar las medidas razonables para validar que su recabado desde el prestador de *Cloud* es completo y preciso, en especial cuando no hay procesos normales de negocio disponibles, y se utilizan medidas específicas de litigación para obtener la información. Es un proceso distinto y separado de la verificación, es decir, que los datos almacenados en *Cloud* sean precisos, estén autenticados o sean admisibles.

3.3.5.5 No accesibles de forma razonable

Debido a las diferencias en el modo en que los datos de un cliente están almacenados y en los derechos y privilegios de acceso de dicho cliente, no todos los datos de clientes almacenados en *Cloud* son accesibles de la misma manera. El cliente (y el prestador) deberían analizar la relevancia, materialidad, proporcionalidad y accesibilidad de las peticiones de información y de la estructura de datos pertinente.

3.3.6 Acceso Directo

Fuera del entorno *Cloud*, el acceso directo por el solicitante al entorno TI de la parte requerida no suele concederse. En el entorno *Cloud*, todavía se concede menos y puede ser imposible por las mismas razones expuestas al hablar de análisis forense. Es importante destacar que un cliente quizás no puede facilitar acceso directo porque el hardware y las instalaciones están fuera de su posesión, custodia o control, y el solicitante necesitaría una citación o negociar directamente con el prestador.

3.3.7 Producción nativa

Los prestadores de servicios *Cloud* almacenan a menudo los datos en sistemas propietarios y aplicaciones en *Cloud* que los clientes no controlan. La producción de datos en formatos nativos puede resultar inútil para los solicitantes, dado que no podrían entender la información producida. En tales circunstancias, lo mejor para todos los afectados - solicitante, parte requerida y prestador- podría ser exportar la información relevante utilizando protocolos estandarizados de realización de informes o de exportación, que existan en el entorno de *Cloud*.

3.3.8 Autenticación

Por autenticación, en este contexto, se entiende la autenticación forense de datos que se admita como prueba. No debe ser confundida con la autenticación de usuarios, que es un componente de la gestión de identidades. Almacenar datos en *Cloud* no afecta al análisis para la autenticación de los datos, para determinar si deben ser admitidos como prueba. La cuestión es si el documento es el que pretende ser. Un correo electrónico no es más o menos auténtico por estar almacenado tras el firewall de una empresa o en *Cloud*. La cuestión es si se ha almacenado con integridad, y si el tribunal confía en que no ha sido alterado desde que fue enviado o recibido.

3.3.9 Admisibilidad y credibilidad

A falta de otra prueba, como la manipulación o el hackeo, los documentos no deberían ser considerados más o menos creíbles o admisibles por haber sido creados o almacenados en *Cloud*.

3.3.10 Cooperación entre el prestador y el cliente en eDiscovery

Resulta del mayor interés, tanto para los prestadores como para los clientes, prever las complicaciones que puede causar el Discovery desde el inicio de la relación, y tenerlo en cuenta en sus ANS. Los prestadores pueden estar interesados en diseñar sus ofertas *Cloud* incluyendo servicios de Discovery, para atraer clientes (“Discovery by Design”). En cualquier caso, clientes y prestadores deberían plantearse incluir en sus acuerdos cláusulas para cooperar mutuamente en caso de peticiones de Discovery contra cualquiera de ellos.

3.3.11 Respuesta a una Citación o a una Orden de Búsqueda

El prestador de servicios *Cloud* puede recibir, de terceros, una petición de facilitar información, en forma de citación, una orden, o disposición judicial en la que se solicite acceso a los datos de un cliente. Al cliente le puede interesar

recurrir tal petición de acceso, a los efectos de proteger la confidencialidad o el secreto de los datos en cuestión. Para ello, los acuerdos de prestación de servicios *Cloud* deberían exigir a los prestadores de servicios *Cloud* comunicar a la empresa que se ha recibido una citación y dar tiempo a dicha empresa a recurrir la petición de acceso.

El prestador de servicios podría estar tentado a responder a la petición abriendo sus instalaciones y facilitando a los solicitantes toda la información incluida en la petición de acceso. Antes de hacerlo, el prestador de servicios *Cloud* debe asegurarse de que la petición está en regla, y cursada siguiendo el procedimiento correcto. El prestador de servicios *Cloud* debe analizar minuciosamente la petición antes de ceder información bajo su custodia.

Dependiendo de la naturaleza específica de la información, o de su localización, por ejemplo, serán de aplicación leyes más o menos complejas. Por ejemplo, son diferentes las normas aplicables por una petición de acceso al contenido de un correo electrónico, en función de si éste ha sido abierto o no, y del tiempo que lleve almacenado. También son diferentes las normas aplicables en función de si la información solicitada es el contenido del mensaje, o únicamente los datos de tráfico del correo electrónico (por ejemplo, quién lo envía, a qué destinatarios, etc.).

DOMINIO 4 //

CUMPLIMIENTO LEGAL Y GESTIÓN DE AUDITORÍA

Las organizaciones se enfrentan a nuevos retos cuando migran de centros de datos (CPD) tradicionales a *Cloud*. El cumplimiento, la medición y la comunicación del alineamiento con la legislación vigente con una multitud de regulaciones en diferentes jurisdicciones es uno de los mayores retos. Tanto clientes como proveedores necesitan comprender y apreciar las diferencias e implicaciones en los estándares de auditoría, procesos y prácticas de cumplimiento legal existentes. La naturaleza distribuida y virtualizada de *Cloud* requiere un ajuste significativo del marco de referencia respecto a aproximaciones basadas en instancias físicas de información y procesos.

Cloud tiene el potencial para mejorar la transparencia y la garantía a través de sus plataformas de gestión más centralizadas y consolidadas. Además, las soluciones de externalización de proveedores *Cloud* reducen la escala y dependencia del cumplimiento legal. Si se cuenta con proveedores capaces de proporcionar soluciones que cumplan la legislación desde el primer momento, nuevas compañías (con y sin ánimo de lucro) podrían entrar en los mercados y realizar acciones que hubieran sido prohibitivas desde un punto de vista económico en la era *pre-Cloud*. Los Gobiernos y otras organizaciones anteriormente en contra de externalizar sus operaciones de TI por cuestiones de seguridad y cumplimiento legal podrían estar más dispuestas a adoptar un modelo de *Cloud*, donde el cumplimiento normativo puede ser ampliamente cubierto a través de la delegación contractual.

Además de proveedores y clientes, los reguladores y auditores se están ajustando a este nuevo mundo de *Cloud Computing*. Pocas de las regulaciones existentes han sido redactadas teniendo en cuenta entornos virtualizados o casos de uso de *Cloud*. Un cliente de *Cloud* puede ser requerido para mostrar a los auditores que su organización cumple con la ley. Comprender la interacción entre *Cloud Computing* y el entorno legislativo es clave para cualquier estrategia *Cloud*. Los clientes *Cloud* deben considerar y comprender lo siguiente:

- Las implicaciones de las regulaciones al usar un servicio Cloud en concreto, prestando especial atención a cualquier aspecto que suponga el traspaso de fronteras o cuestiones multi-jurisdiccionales.
- La asignación de responsabilidades de cumplimiento legal entre el proveedor y el cliente, incluyendo proveedores indirectos (por ejemplo, el proveedor Cloud de tu proveedor Cloud).
- La capacidad del proveedor de demostrar cumplimiento legal, incluyendo la generación de documentación, producción de evidencias y los procesos de conformidad normativa en un tiempo razonable.
- Las relaciones entre los clientes, proveedores y auditores (tanto los del cliente como los del proveedor) para garantizar el acceso necesario (y restringido, donde se precise) y el alineamiento con las necesidades de gobierno.

Introducción. Este dominio incluye:

- Cumplimiento legal
- Auditoría

4.1 Cumplimiento legal



Figura 7— Ecosistema de valor GRC

- **Gobierno Corporativo:** el equilibrio de control entre las personas interesadas, directores y ejecutivos de una organización que proporciona una dirección consistente, una aplicación de políticas coherente, guías y controles que facilitan una toma de decisiones efectiva.
- **Gestión de Riesgo Empresarial:** métodos y procesos (marco de referencia) usado por las organizaciones para equilibrar la toma de decisiones basada en identificar eventos concretos o circunstancias relevantes para los objetivos de la organización (riesgos y oportunidades), considerándolos en términos de probabilidad y magnitud del impacto, determinando una estrategia de respuesta y monitorizando el progreso para proteger y crear valor para las partes interesadas.
- **Cumplimiento legal y garantía de auditoría:** concienciación y adhesión a las obligaciones empresariales (por ejemplo, responsabilidad social corporativa, ética, legislación aplicable, regulaciones, contratos, estrategias y políticas) a través del conocimiento del estado del cumplimiento legal, evaluación de riesgos y los costes potenciales del incumplimiento frente a los costes del cumplimiento normativo y, en consecuencia, priorizar, fomentar e iniciar cualquier acción correctiva que fuera precisa.

Las tecnologías de la información en *Cloud* están sujetas a una creciente exposición a más políticas y regulaciones. Todas las partes interesadas esperan que las organizaciones cumplan proactivamente con las normas regulatorias en múltiples jurisdicciones legales. El Gobierno TI requiere ejercer su función teniendo en cuenta estos requerimientos y todas las compañías precisan una estrategia para ello.

El Gobierno incluye los procesos y políticas que facilitan la consecución sencilla de los objetivos empresariales teniendo en cuenta las limitaciones del entorno externo. El Gobierno requiere actividades de cumplimiento legal que garanticen que las operaciones están plenamente alineadas con esos procesos y políticas. En este sentido, el cumplimiento legal está focalizado en alinearse con los requerimientos externos (por ejemplo, leyes, regulaciones, estándares de la industria) mientras que el Gobierno está focalizada en alinearse con los requerimientos internos (por ejemplo, decisiones del Consejo, política corporativa).

El cumplimiento legal puede ser definido como la concienciación y seguimiento de las obligaciones (por ejemplo, responsabilidad social corporativa, leyes aplicables, guías éticas), incluyendo el conocimiento y la priorización de las acciones correctivas que sean necesarias y apropiadas. En algunos entornos, y especialmente en aquellos que están altamente regulados, la transparencia puede ser dominante, al poner más atención en la obligación de informar que en el propio cumplimiento. En las mejores circunstancias, el cumplimiento legal no es un inhibidor de la efectividad organizacional sino un complemento a determinadas políticas internas.

Habitualmente las regulaciones tienen implicaciones serias para las tecnologías de la información y su Gobierno, especialmente en términos de monitorización, gestión, protección y divulgación. El Gobierno TI es un elemento de apoyo para todo el Gobierno corporativo, Gestión de Riesgo empresarial, Cumplimiento Legal y Auditoría/Garantía.

Cloud puede ser una tecnología facilitadora para el Gobierno y el Cumplimiento Legal, centralizando el control y la transparencia a través de sus plataformas de gestión, particularmente para *Cloud* gestionado internamente. Mediante el impulso de los servicios *Cloud*, organizaciones de diferentes tamaños pueden obtener el mismo nivel de cumplimiento legal que entidades más grandes y con más recursos. Los servicios de seguridad y garantía son una de las maneras por las que terceras empresas pueden jugar un papel importante en la valoración y comunicación del cumplimiento legal.

Cualquier aproximación al cumplimiento legal necesitará contar con la participación de toda la organización, incluyendo a TI. El papel de los proveedores externos debe ser considerado con cautela y la responsabilidad de incluirlos en el área de Gobierno, directa o indirectamente, debe ser explícitamente asignada dentro de la organización del cliente.

Adicionalmente, se presenta a continuación un listado de estándares de seguridad *Cloud* que se encuentran en desarrollo en ISO/IEC y ITU-T:

- ISO/IEC 27017: Seguridad en *Cloud Computing* y Sistema de Gestión de la Seguridad y Controles de Privacidad.
- ISO/IEC 27036-x: Estándar multiparte para la gestión de la seguridad de la información del proveedor que está previsto que incluya una parte relevante a la cadena de suministro *Cloud*.
- ITU-T X.ccsec: Guía de seguridad para *Cloud Computing* en el área de Telecomunicaciones.
- ITU-T X.srfcts: Requerimientos de seguridad y marco de referencia para entornos de servicios de telecomunicaciones (X.srfcts).
- ITU-T X.sfcse: Requerimientos de seguridad funcionales para entornos de aplicaciones SaaS.

4.2 Auditoría

Un Gobierno corporativo adecuada incluye auditorías y garantías. La auditoría debe ser llevada a cabo de manera independiente y debe estar diseñada de forma robusta para reflejar las buenas prácticas, recursos apropiados y protocolos y estándares revisados.

Tanto la auditoría interna como la externa y sus controles correspondientes juegan un papel importante en *Cloud*, tanto para el cliente como para el proveedor. Durante las etapas iniciales de la introducción de *Cloud* la transparencia es todavía más evidente para incrementar los niveles de confort de las partes interesadas. La auditoría es un método que proporciona garantía de que las actividades de gestión del riesgo operacional han sido comprobadas y revisadas en profundidad.

El plan de auditoría debe ser adoptado y apoyado por los responsables ejecutivos de la organización (el Consejo y la dirección ejecutiva). La existencia y ejecución de auditorías independientes y planificadas de los sistemas críticos y controles, que incluyan trazabilidad de acciones y documentación, ayudará a mejorar en eficiencia y confiabilidad.

Muchas organizaciones usan un modelo de madurez (por ejemplo, CMM, PTQM) como marco de referencia para analizar la efectividad de los procesos. En algunos casos, puede adoptarse una aproximación más estadística a la gestión de riesgo (por ejemplo, los acuerdos Basilea y Solvencia para los servicios financieros) y cuando este espacio madure, podrán adoptarse otros modelos más especializados de riesgo en función de las necesidades requeridas para la línea de negocio.

Para *Cloud*, estas prácticas necesitarán ser revisadas y mejoradas. Tal como ocurría con los modelos previos de tecnologías de la información, la auditoría necesitará aprovechar las ventajas del potencial de *Cloud*, así como incrementar el alcance y escala que faciliten la gestión de las áreas menos maduras.

4.3 Recomendaciones

Cuando se establece contacto con un proveedor, se debe involucrar a los correspondientes equipos de legal, compras y contratación de la organización del cliente. Los términos estándar de servicio podrían no cubrir las necesidades de cumplimiento legal y deberían ser negociados.

Algunos requerimientos de cumplimiento legal específicos para industrias altamente reguladas (por ejemplo, entornos financieros o sanidad) deben ser tenidos en cuenta cuando se plantea un servicio *Cloud*. Las organizaciones que entienden sus requerimientos actuales deben plantearse el impacto de un modelo de TI distribuido, incluyendo el impacto de diversos proveedores *Cloud* operando en diferentes ubicaciones geográficas y diferentes jurisdicciones legales.

Se debe determinar cómo el uso de servicios Cloud impacta en los actuales requerimientos de cumplimiento legal para cada carga de trabajo (por ejemplo, un conjunto de aplicaciones y datos), en particular en lo que se refiere a la seguridad de la información. Como con cualquier solución de externalización, las organizaciones necesitan comprender cuáles son sus proveedores *Cloud* y si tratarán con información sujeta a regulaciones. Algunos ejemplos de políticas y procedimientos impactados incluyen informes de actividad, monitorización de eventos, retención de la información, respuesta a incidentes y políticas de privacidad.

Comprender las responsabilidades contractuales de cada parte. Las expectativas variarán de un modelo de despliegue a otro, con el cliente teniendo más control y responsabilidad en un modelo IaaS, y el proveedor cogiendo el rol dominante para la soluciones SaaS. Particularmente importantes son los requerimientos encadenados y obligaciones, no solo del cliente y su proveedor *Cloud* sino también entre el usuario final y el proveedor de su proveedor *Cloud*.

El cumplimiento legal (leyes, requisitos legales técnicos, cumplimiento, riesgo y seguridad) es crítico y debe considerarse en la fase de identificación de requerimientos. Cualquier información procesada, transmitida, almacenada o visualizada que sea considerada Información Personal Identificable (**PII**, por sus siglas en inglés)¹⁶ o información privada, se enfrenta a una plétora de regulaciones y normativas en todo el mundo que varían entre países y estados. Debido a que la tecnología *Cloud* fue diseñada para ser geográficamente diversa y escalable, los datos pueden ser almacenados, procesados, transmitidos o recuperados desde diversas localizaciones o múltiples CPDs del proveedor de servicios *Cloud*.

¹⁶ PII - *Personal Identifiable Information*; datos de carácter personal.

Algunos requerimientos regulatorios especifican controles que son difíciles o imposibles de cumplir en ciertos tipos de servicios *Cloud* (por ejemplo, los requerimientos geográficos pueden ser inconsistentes con el almacenamiento distribuido). Clientes y proveedores deben acordar cómo se recogen, almacenan y comparten evidencias electrónicas para el cumplimiento legal (por ejemplo, logs de auditoría, informes de actividad, configuraciones de sistemas).

- Es preferible disponer de auditores que conozcan el ámbito *Cloud* y que estén familiarizados con los retos de garantías (y ventajas) de la virtualización y de *Cloud*.
- Solicite informes a su proveedor SSAE 16 SOC2 o ISAE 3402 Tipo 2. Estos aportan un inequívoco punto de arranque como referencia para auditores y asesores.
- Los contratos deben facilitar una revisión por un tercero de las métricas y acuerdos de niveles de servicios del cumplimiento legal (por ejemplo, por un mediador seleccionado por ambas entidades).

4.4 Requerimientos

- ✓ Una cláusula de derecho a auditar aporta a los clientes la capacidad de auditar al proveedor *Cloud* y apoya la trazabilidad y transparencia en los frecuentes entornos cambiantes de la regulación en *Cloud*. Utilice una normativa como base al auditar para asegurarse el mutuo conocimiento de las expectativas. En el momento adecuado, este derecho se verá sustituido por certificaciones de terceros (por ejemplo, a través de ISO/IEC 27001/27017).
- ✓ Una cláusula de derecho a la transparencia con accesos específicos puede dar al cliente la información necesaria en industrias altamente reguladas (incluso en aquellas donde la no-conformidad legal puede ser base para procesamiento criminal). El acuerdo debe distinguir entre acceso directo/automático a la información (por ejemplo, logs, informes) e información 'enviada' (por ejemplo, arquitecturas de sistemas, informes de auditoría).
- ✓ Los proveedores deben revisar, actualizar y publicar sus documentos de información de seguridad y procesos GRC de manera regular (o cuando se les requiera). Estos deben incluir análisis de vulnerabilidades y las actividades relacionadas de subsanación.
- ✓ Los auditores de terceros deben ser mutuamente reconocidos o escogidos de manera anticipada, conjuntamente por el proveedor y el cliente.
- ✓ Todas las partes implicadas deben acordar el uso de un marco de referencia común para la certificación y garantía (por ejemplo, de ISO, COBIT) para el Gobierno TI y controles de seguridad.

DOMINIO 5 //

GESTIÓN DE LA INFORMACIÓN Y DE LA SEGURIDAD DE LOS DATOS

El objetivo principal de seguridad de la información es proteger los datos fundamentales que alimentan nuestros sistemas y aplicaciones. A medida que las empresas evolucionan hacia *Cloud computing*, los métodos tradicionales para proteger los datos son desafiados por las arquitecturas basadas en *Cloud*. La elasticidad, *multitenancy*, las nuevas arquitecturas físicas y lógicas, y los controles abstractos requieren nuevas estrategias de seguridad de datos. En muchas implementaciones de *Cloud*, los usuarios incluso transfieren datos a entornos externos, o incluso públicos, de formas que hubieran sido impensables pocos años atrás.

Gestionar información en la era de *Cloud computing* es un desafío de enormes proporciones que afecta a todas las organizaciones, incluso a aquellas que no parecen estar implicadas activamente en proyectos basados en *Cloud*. Comienza con la gestión de los datos internos y las migraciones a *Cloud* y se extiende a proteger la información en aplicaciones y servicios que afectan de forma difusa a más de una organización. La gestión de la información y la seguridad de los datos en la era *Cloud* demanda tanto estrategias como arquitecturas técnicas nuevas. Afortunadamente, no sólo los usuarios tienen las herramientas y técnicas necesarias, sino que la transición a *Cloud* incluso crea oportunidades para mejorar la seguridad de los datos en nuestra infraestructura tradicional.

Los autores recomiendan utilizar un 'ciclo de vida de la seguridad de los datos' (analizado más adelante) para evaluar y definir la estrategia de seguridad de datos en *Cloud*. Ésta debe ser en capas con unas políticas claras de gobierno de la información, y a continuación, aplicada mediante las tecnologías clave, tales como el cifrado y herramientas especializadas de monitorización.

Introducción. Este dominio incluye tres secciones:

- La sección 1 proporciona material de referencia sobre arquitecturas de información (almacenamiento) en *Cloud*.
- La sección 2 incluye las mejores prácticas de gestión de la información, incluyendo el ciclo de vida de seguridad de los datos.
- La sección 3 detalla controles específicos de seguridad de los datos y cuándo utilizarlos.

5.1 Arquitecturas de información *Cloud*

Las arquitecturas de información en *Cloud* son tan diversas como las propias arquitecturas de *Cloud*. Si bien esta sección no puede cubrir todas las combinaciones posibles, hay ciertas arquitecturas comunes a la mayoría de los servicios de *Cloud*.

5.1.1 IaaS

IaaS, para un cloud público o privado, incluye generalmente las siguientes opciones de almacenamiento:

- **Almacenamiento puro.** Incluye los medios físicos donde los datos están almacenados. Se pueden mapear para acceso directo en ciertas configuraciones de *cloud* privado.

- **Almacenamiento de volúmenes.** Incluye los volúmenes asociados a instancias IaaS, normalmente como *discos duros virtuales*. Los volúmenes usan frecuentemente dispersión de datos para proporcionar robustez y seguridad.
- **Almacenamiento de objetos.** El almacenamiento de objetos se denomina, en ocasiones, almacenamiento de ficheros. Más que un disco duro virtual, el almacenamiento de objetos se parece más a un fichero compartido accedido mediante **APIs** o un interfaz web.
- **Red de distribución de contenidos (CDN).** El contenido se ubica en un almacenamiento de objetos, el cual se distribuye a múltiples nodos repartidos geográficamente para mejorar las velocidades de consumo desde Internet.

5.1.2 PaaS

PaaS proporciona y se apoya en un amplio abanico de opciones de almacenamiento.

PaaS puede proporcionar:

- **Database as a Service (DaaS).** Una arquitectura de base de datos *multitenant* que se puede usar directamente como servicio. Los usuarios la usan vía APIs o directamente mediante llamadas **SQL**¹⁷, dependiendo de lo que se ofrezca. Los datos de cada cliente están segregados y aislados del resto. Las bases de datos pueden ser relacionales, planas o con cualquier otra estructura común.
- **Hadoop/MapReduce/Big Data as a Service.** *Big Data* son datos cuya gran escala, amplia distribución, heterogeneidad, y actualidad requieren el uso de nuevas arquitecturas técnicas y analíticas. *Hadoop* y otras aplicaciones *Big Data* pueden ser ofrecidas como una plataforma *cloud*. Los datos se ubican en un *almacenamiento de objetos* o en otro sistema distribuido de ficheros. Los datos normalmente han de estar cerca del entorno de procesado, y pueden ser movidos temporalmente a medida que se necesita para su procesado.
- **Almacenamiento para aplicaciones.** El almacenamiento para aplicaciones cubre cualquier opción de almacenamiento incluida en una plataforma de aplicación PaaS y consumible mediante APIs y que no encaja en ninguna de las otras categorías de almacenamiento.

PaaS puede consumir:

1. **Bases de datos.** La información y el contenido pueden ser almacenados directamente en la base de datos (como texto u objeto binario) o como ficheros referenciados por la base de datos. La base de datos misma puede ser una colección de instancias IaaS compartiendo un *back-end* de almacenamiento común.
2. **Almacenamiento de Objetos/Ficheros.** Los ficheros u otros datos se ubican en un almacenamiento de objetos, pero solo son accedidos mediante el API del PaaS.
3. **Almacenamiento de volúmenes.** Los datos pueden estar almacenados en volúmenes IaaS asociados a instancias dedicadas al servicio PaaS.

¹⁷ **SQL** - *Structural Query Language* es un lenguaje de programación diseñado para el manejo de datos

4. **Otros.** Estos son los modelos de almacenamiento más comunes, pero es un área dinámica y pueden estar disponibles otras opciones.

5.1.3 SaaS

Al igual que PaaS, SaaS usa una amplia gama de modelos de almacenamiento y uso. Siempre se accede al almacenamiento SaaS mediante un interfaz de usuario basado en web o una aplicación cliente/servidor. Si se accede al almacenamiento mediante API, se considera PaaS. Muchos proveedores SaaS proporcionan también esas APIs PaaS.

SaaS puede proporcionar:

- **Almacenamiento y gestión de la información.** Los datos se introducen en el sistema mediante un interfaz web y se almacenan en la aplicación SaaS (normalmente una base de datos de *back-end*). Algunos servicios SaaS ofrecen opciones para subir conjuntos de datos, o APIs PaaS.
- **Almacenamiento de Contenido/Ficheros.** El contenido basado en ficheros se almacena en la aplicación SaaS (por ejemplo informes, ficheros de imágenes, documentos) y se proporciona acceso mediante un interfaz de usuario basado en web.

SaaS puede consumir:

- **Bases de datos.** Al igual que PaaS, un gran número de Servicios SaaS se apoyan en bases de datos de *back-end*, incluso para almacenamiento de ficheros.
- **Almacenamiento de Objetos/Ficheros.** Los ficheros y otros datos se guardan en almacenamiento de objetos, pero solo son accedidos mediante la aplicación SaaS.
- **Almacenamiento de volúmenes.** Los datos pueden ser almacenados en volúmenes IaaS asociados a instancias dedicadas a proporcionar el servicio SaaS.

5.2 Dispersión de Datos (Información)

La dispersión de datos (información) es una técnica usada habitualmente para mejorar la seguridad de los datos, pero sin el uso de mecanismo de cifrado. Este tipo de algoritmos (**IDA**¹⁸ para abreviar) permiten proporcionar alta disponibilidad y asegurar los datos almacenados en *Cloud*, por medio de la fragmentación de datos, y son comunes en muchas plataformas *Cloud*. En un esquema de fragmentación, un fichero f se trocea en n fragmentos; todos los cuales se firman y distribuyen a n servidores remotos. El usuario puede entonces reconstruir f accediendo m fragmentos arbitrariamente escogidos. El mecanismo de fragmentación puede también usarse para almacenar datos de larga duración con un alto nivel de aseguramiento en *Cloud*.

Cuando se usa la fragmentación junto con el cifrado, la seguridad de los datos mejora: un adversario ha de comprometer m nodos para poder obtener m fragmentos del fichero f , y entonces ha de romper el mecanismo de cifrado usado.

¹⁸ IDA - Intrusion Detection Algorithms

5.3 Gestión de la información

Antes de poder revisar los controles específicos de seguridad de los datos, se necesita un modelo para entender y gestionar la información. La gestión de la información incluye los procesos y políticas para entender cómo se usa la información y cómo se gobierna su uso. En la sección de seguridad de los datos, se revisan los controles técnicos específicos y las recomendaciones para monitorizar y aplicar este gobierno.

5.4 El Ciclo de vida de la seguridad de los datos

Aunque la gestión del ciclo de vida de la información es un campo maduro, no encaja bien con las necesidades de los profesionales de la seguridad. El ciclo de vida de la seguridad de los datos es diferente de la gestión del ciclo de vida de la información, reflejando las diferentes necesidades de los profesionales de la seguridad. Resumimos aquí el ciclo de vida, cuya versión completa está disponible en <http://www.secuosis.com/blog/data-security-lifecycle-2.0>

El ciclo de vida incluye seis fases, desde la creación a la destrucción. Aunque se muestra como una progresión lineal, una vez creados, los datos pueden moverse entre fases sin restricciones, y puede que no pasen por todas las etapas (por ejemplo, no todos los datos son finalmente destruidos).

- **Creación.** Creación es la generación de nuevo contenido digital, o la alteración, actualización o modificación de contenido existente.
- **Almacenamiento.** Almacenamiento es el acto de ubicar los datos digitales en algún tipo de repositorio de almacenamiento y normalmente ocurre de forma prácticamente simultánea a su creación.
- **Uso.** Los datos son visualizados, procesados, o utilizados de otro modo en algún tipo de

actividad, no incluyendo su modificación.

- **Compartición.** La información se hace accesible a otros, tales como otros usuarios, clientes, y colaboradores.
- **Archivado.** Los datos dejan de ser usados activamente y entran en un almacenamiento de largo plazo.
- **Destrucción.** Los datos son destruidos de forma permanente usando medios físicos o digitales (por ejemplo, *crypto shredding*).



Figura 8- Ciclo de Vida de Seguridad de los Datos

5.4.1 Localización y Acceso

El ciclo de vida representa las fases por las que la información pasa, pero no cubre su localización ni cómo son accedidos.

Localizaciones

La importancia de las localizaciones se puede ilustrar pensando en el ciclo de vida no como una operación única y lineal, sino como una serie de ciclos de vida más pequeños, funcionando en diferentes entornos operativos. Los datos pueden moverse prácticamente, en cada fase, dentro, fuera o entre esos entornos.

Debido a las potenciales cuestiones regulatorias, contractuales, y jurisdiccionales es extremadamente importante entender tanto la localización lógica como física de los datos.

Accesos

Una vez que los usuarios saben dónde residen los datos y cómo se mueven, necesitan saber quién está accediendo a ellos y cómo. Aquí entran dos factores:

1. ¿Quién accede a los datos?
2. ¿Cómo pueden acceder a ellos (dispositivo y canal)?

Actualmente se accede a los datos mediante una variedad de dispositivos. Estos dispositivos tienen diferentes características de seguridad y pueden utilizar diferentes aplicaciones o clientes.

5.4.2 Funciones, Actores, y Controles

El siguiente paso es identificar las funciones que pueden ser realizadas con los datos, por un actor (persona o sistema) dado y en una localización concreta.

Funciones

Hay tres cosas que se pueden hacer con un dato dado:

- **Acceder.** Ver/acceder al dato, incluyendo crearlo, copiarlo, transferir el fichero, diseminarlo, y otros intercambios de información.
- **Tratar.** Realizar una transacción con el dato: actualizarlo, usarlo en una transacción de un proceso de negocio, etc.
- **Almacenar.** Guardar el dato (en un fichero, base de datos, etc.).

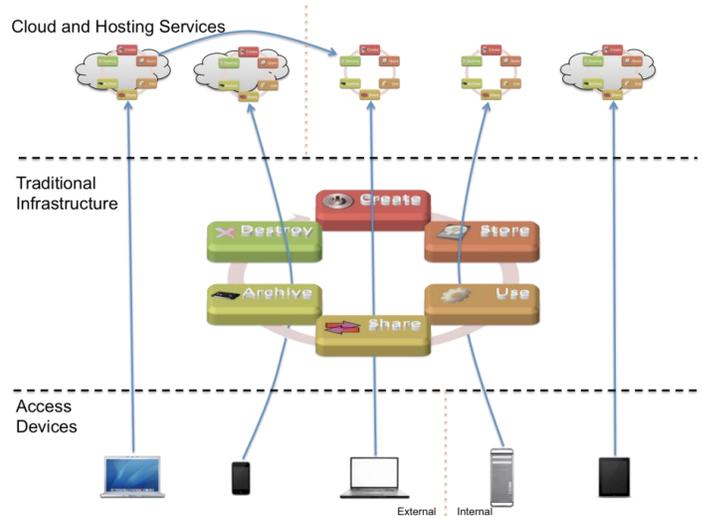


Figura 9- Ciclo de Vida de Seguridad de los Datos. Localizaciones y Acceso

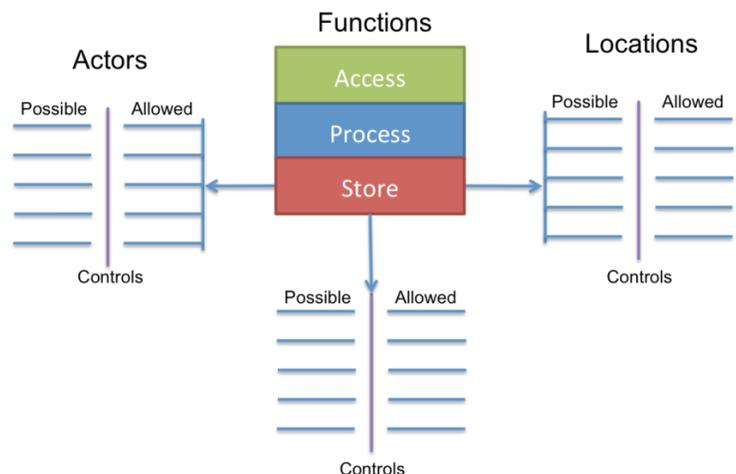


Figura 10- Ciclo de Vida de Seguridad de los Datos. Funciones, Actores y Controles

La siguiente tabla muestra qué funciones encajan con qué fases del ciclo de vida:

Tabla 4—Fases del ciclo de vida de la información

	Crear	Almacenar	Usar	Compartir	Archivar	Destruir
Acceso	X	X	X	X	X	X
Tratamiento	X		X			
Almacenamiento		X			X	

Un *actor* (persona, aplicación, o sistema/proceso, como opuesto a un dispositivo de acceso) realiza cada función en una *localización*.

Controles

Un *control* restringe una lista de *posibles* acciones a las acciones *permitidas*. La siguiente tabla muestra una forma de listar las posibilidades, las cuales debe mapear el usuario con los controles.

Tabla 5—Controles posibles y permitidos

Función		Actor		Localización	
Posible	Permitido	Posible	Permitido	Posible	Permitido

5.5 Gobierno de la Información

El gobierno de la información incluye las políticas y procedimientos para gestionar el uso de la información. Incluye las siguientes características clave:

- **Clasificación de la información.** Descripciones de alto nivel de las categorías principales de la información. A diferencia de la *clasificación de datos* el objetivo no es etiquetar cada pedazo de información en la organización, sino definir categorías de alto nivel tales como “regulado” y “secreto comercial” para determinar qué controles de seguridad se pueden aplicar.
- **Políticas de gestión de la información.** Políticas para definir qué actividades se permiten para los distintos tipos de información.
- **Políticas jurisdiccionales y de localización.** Dónde se pueden ubicar geográficamente los datos, lo cual tiene importantes ramificaciones legales y regulatorias.
- **Autorizaciones.** Definir qué tipos de empleados/usuarios tienen permisos para acceder a qué tipos de información.
- **Propiedad.** Quién es el responsable final de la información.
- **Custodia.** Quién es el responsable de la gestión de la información, a petición del propietario.

5.6 Seguridad de los datos

La seguridad de los datos incluye los controles y tecnologías específicas utilizadas para garantizar el cumplimiento del gobierno de la información. Se ha dividido en tres secciones para tratar la detección (y prevención) en la migración de datos a *Cloud*, proteger los datos en el tránsito a *Cloud* entre diferentes proveedores/entornos, y proteger los datos una vez que están en *Cloud*.

5.6.1 Detección y prevención en la migración de datos a *Cloud*

Un problema común que afrontan las organizaciones en *Cloud* es la gestión de los datos. Muchas organizaciones informan de que las personas o las unidades de negocio migran frecuentemente datos delicados a *Cloud* sin la aprobación o incluso sin haber informado a TI o a seguridad.

Además de los controles tradicionales de seguridad de los datos (como controles de acceso o cifrado), hay otros dos pasos que ayudan a gestionar la migración no autorizada de datos a servicios *Cloud*:

1. Monitorizar la existencia de grandes movimientos internos de datos con herramientas de monitorización de actividad de bases de datos (**DAM**)¹⁹ y de monitorización de actividad en ficheros (**FAM**)²⁰.
2. Monitorizar la migración de datos a *Cloud* con filtros URL y herramientas *Data Loss Prevention*.

Migraciones internas de datos

Antes de que los datos se puedan migrar a *Cloud* necesitan ser extraídos de sus repositorios. Las herramientas DAM pueden detectar cuándo un administrador u otro usuario extrae grandes conjuntos de datos o replica una base de datos, lo cual puede ser un indicio de una migración.

Las herramientas FAM proporcionan una protección similar para los repositorios de ficheros, como las carpetas compartidas.

Migración al *Cloud*

Una combinación de filtrado de URL (pasarelas web de seguridad de contenidos) y herramientas DLP pueden detectar la migración de datos de la empresa a *Cloud*.

El filtrado de URL permite vigilar (y evitar) la conexión de los usuarios a servicios *Cloud*. Dado que las interfaces de administración de estos servicios suelen utilizar direcciones distintas a las de uso, el usuario puede distinguir entre alguien que accede a una consola de administración, frente a un usuario que accede a una aplicación ya alojada con el proveedor.

Se ha de buscar una herramienta que ofrezca una lista de servicios *Cloud* y la mantenga al día, frente a una que requiera la creación de una categoría personalizada, y que el usuario gestione las direcciones destino.

¹⁹ **DAM** - Database Activity Monitoring

²⁰ **FAM** - File Activity Monitoring

Para una mayor granularidad, se ha de utilizar DLP. Las herramientas DLP vigilan los datos/contenidos reales que se transmiten, no sólo el destino. Así, el usuario puede generar alertas (o bloqueos) basados en la clasificación de los datos. Por ejemplo, el usuario puede permitir que datos privados empresariales vayan a un servicio *Cloud* aprobado, pero bloquear la migración del mismo contenido a un servicio no autorizado.

El punto de inserción de la solución de DLP puede determinar el éxito en la detección de la fuga de datos. Por ejemplo, la disponibilidad de soluciones *Cloud* para usuarios diferentes (por ejemplo, empleados, proveedores, clientes) fuera del entorno de red corporativa evita o anula cualquier solución DLP si se inserta en el perímetro de la empresa.

5.6.2 Proteger la migración de datos a (o en) el *Cloud*

En las implementaciones de *Cloud* públicas y privadas, y a través de los diferentes modelos de servicio, es importante proteger los datos en tránsito. Esto incluye:

- Los datos moviéndose desde la infraestructura tradicional a los proveedores *Cloud*, incluyendo público/privado, interior/exterior y otras combinaciones.
- Los datos migrando entre los proveedores de *Cloud*.
- Los datos moviéndose entre instancias (u otros componentes) en un *Cloud* determinado.

Hay tres opciones (por orden de preferencia):

1. **Cifrado Cliente/Aplicación.** Los datos son cifrados en el extremo o en el servidor antes de enviarse por la red o ya están almacenados en un formato de cifrado adecuado. Esto incluye el cifrado en cliente local (basado en agente), por ejemplo para ficheros almacenados, o el cifrado integrado en aplicaciones.
2. **Cifrado Enlace/Red.** Técnicas de cifrado de red estándar incluyendo SSL²¹, VPNs²², y SSH²³. Puede ser hardware o software. Es preferible extremo a extremo pero puede no ser viable en todas las arquitecturas.
3. **Cifrado basado en Proxy.** Los datos son transmitidos a un servidor dedicado o servidor proxy, el cual los cifra antes de enviarlos por la red. Es la opción escogida frecuentemente para la integración con aplicaciones *legacy* pero no es generalmente recomendable.

5.6.3 Protección de los datos en *Cloud*

Dada la amplia gama de opciones y tecnologías disponibles en *Cloud computing*, no hay una forma de cubrir todas las posibles opciones de seguridad. A continuación se tratan algunas de las tecnologías más útiles y de las mejores prácticas para proteger los datos dentro de varios modelos de *Cloud*.

5.6.3.1 Localización de contenidos

La localización de contenidos incluye las herramientas y procesos para identificar aquella información delicada que esté almacenada. Permite que la organización defina políticas basadas en el tipo de información, estructura, o clasificación y escanea los datos almacenados mediante técnicas avanzadas de análisis de contenido para identificar localizaciones y violaciones de las políticas.

²¹ SSL; Secure Sockets Layer

²² Virtual Private Networks

²³ Secure SHell

La localización de contenidos es normalmente una funcionalidad de las herramientas de *Data Loss Prevention*; para bases de datos, está disponible en ocasiones en los productos de monitorización de la actividad de bases de datos (DAM). El escaneo puede hacerse accediendo a las carpetas compartidas o mediante un agente instalado en el sistema operativo. La herramienta ha de ser “*Cloud aware*”, es decir, capaz de trabajar en entorno *Cloud* (por ejemplo, capaz de escanear un almacenamiento de objetos). La localización de contenidos puede estar también disponible como servicio gestionado.

5.6.3.2 Cifrado IaaS

5.6.3.2.1 Cifrado de almacenamiento de volúmenes

El cifrado de volúmenes protege de los siguientes riesgos:

- Protege los volúmenes de su exposición a un clonado mediante *snapshot*.
- Protege a los volúmenes de ser explorados por el proveedor *Cloud* (y los administradores de *Cloud* privados)
- Protege a los volúmenes de verse expuestos ante una pérdida física de discos (un problema más de cumplimiento que de seguridad real)

Los volúmenes IaaS pueden cifrarse usando tres métodos:

- **Cifrado gestionado por instancias.** El motor de cifrado funciona dentro de la instancia, y la clave se guarda en el volumen pero protegida por una contraseña o un par de claves.
- **Cifrado gestionado externamente.** El motor de cifrado funciona dentro de la instancia, pero las claves se gestionan de forma externa y se proporcionan a la instancia bajo demanda.
- **Cifrado proxy.** En este modelo el volumen se conecta a una instancia especial o *appliance/software*, y entonces se conecta la instancia a una instancia cifrada. El proxy maneja todas las operaciones criptográficas y puede mantener las claves de forma interna o externa.

5.6.3.2.2 Cifrado de almacenamiento de objetos

El cifrado del almacenamiento de objetos protege de muchos de los riesgos presentes en el almacenamiento de volúmenes. Dado que el almacenamiento de objetos es accesible con más frecuencia desde redes públicas, también permite que el usuario implemente un *almacenamiento privado virtual*. Al igual que una VPN, un **VPS**²⁴ permite el uso de una infraestructura pública compartida a la vez que los datos permanecen protegidos, dado que solo quien disponga de las claves de cifrado pueden leer los datos, aunque lleguen a estar expuestos.

- **Cifrado de ficheros/carpetas y Enterprise Digital Rights Management.** Utiliza herramientas de cifrado estándar de ficheros/carpetas o EDRM para cifrar los datos antes de ubicarlos en el almacenamiento de objetos.
- **Cifrado de cliente/aplicación.** Cuando se usa almacenamiento de objetos como el *back-end* de una aplicación (incluyendo aplicaciones móviles), cifra los datos usando un motor embebido en la aplicación o el cliente.
- **Cifrado proxy.** Los datos pasan por un *proxy* de cifrado antes de ser enviado al almacenamiento de objetos.

²⁴ **VPS** - *Virtual Private Storage*. Almacenamiento privado virtual.

5.6.3.3 Cifrado PaaS

Dado que PaaS es tan diverso, la siguiente lista no cubre todas las potenciales opciones:

- **Cifrado de cliente/aplicación.** Los datos se cifran en la aplicación PaaS o por el cliente que accede a la plataforma.
- **Cifrado de base de datos.** Los datos se cifran en la base de datos utilizando cifrado incorporado y soportado por la plataforma de base de datos.
- **Cifrado proxy.** Los datos pasan por un *proxy* de cifrado antes de ser enviados a la plataforma.
- **Otros.** Otras opciones pueden incluir APIs incorporadas en la plataforma, Servicios externos de cifrado, y otras variantes.

5.6.3.4 Cifrado SaaS

Los *proveedores SaaS* pueden usar alguna de las opciones revisadas previamente. Se recomienda, cuando sea posible, el uso de claves diferentes para cada cliente para aplicar mejor el aislamiento *mutitenant*. Las siguientes opciones son para los clientes SaaS:

- **Cifrado gestionado por el proveedor.** Los datos se cifran en la aplicación SaaS y son gestionado habitualmente por el proveedor.
- **Cifrado proxy.** Los datos pasan por el proxy de cifrado antes de enviarse al a la aplicación SaaS.

Las operaciones de cifrado deben usar el método de cifrado que sea más apropiado, lo cual puede incluir claves compartidas o pares de claves pública/privada y una estructura **PKI/PKO**²⁵ (Public Key Infrastructure/Operations). Por favor, revise el Dominio 11 para obtener más información sobre cifrado o gestión de claves.

5.6.4 Data Loss Prevention

Data Loss Prevention (DLP) se define como: “Productos que, basados en políticas centralizadas, identifican, monitorizan, y protegen los datos estáticos, en movimiento, y en uso, mediante un análisis profundo de contenidos”.

DLP puede proporcionar opciones sobre cómo se han de manejar los datos cuando se detecte un incumplimiento de las políticas. Los datos pueden ser bloqueados (detener un flujo de trabajo) o permitidos para continuar tras aplicar mediante cifrado un remedio utilizando métodos como DRM, ZIP, o OpenPGP.

DLP se usa normalmente para el descubrimiento de contenidos y la monitorización de datos en movimiento utilizando las siguientes opciones:

- **Appliance/servidor dedicado.** Hardware estándar ubicado en un cuello de botella entre el entorno *cloud* y el resto de la red/Internet o entre diferentes segmentos *Cloud*.
- **Appliance virtual**

²⁵ **PKI/PKO** - Public Key Infrastructure/Operations, Infraestructura/Operaciones de Clave Pública

- **Agente en el extremo**
- **Agente en hipervisor.** El agente DLP está embebido o se accede al mismo a nivel de hipervisor, en lugar de ejecutarse en la instancia.
- **DLP SaaS.** El DLP está integrado en el servicio *cloud* (por ejemplo, email en *cloud*) u ofrecido como un servicio independiente (normalmente de descubrimiento de contenido).

5.6.5 Monitorización de actividad en bases de datos y en ficheros

La monitorización de actividad en base de datos (DAM) se define como: *“La monitorización de actividad de base de datos captura y registra, como mínimo, toda la actividad Structured Query Language (SQL) en tiempo real o casi real, incluyendo actividad de los administradores, a través de múltiples plataformas de base de datos; y puede generar alertas de incumplimiento de políticas”.*

DAM realiza una monitorización en tiempo casi real de la actividad de las base de datos y alerta en base a incumplimientos de las políticas, tales como ataques de inyección SQL o replicación de la base de datos sin autorización por el administrador. Las herramientas DAM para entorno *Cloud* se basan normalmente en agentes que se conectan a un servidor recolector central (normalmente virtualizado). Se usan con instancias dedicadas a un único cliente, aunque en un futuro puede estar disponible para PaaS.

La monitorización de actividad en ficheros (FAM) se define como: *Productos que monitorizan y registran toda la actividad a nivel de usuario en los repositorios de datos designados, y genera alertas de incumplimiento de políticas.*

FAM para *Cloud* requiere el uso de agentes o ubicar un *appliance* físico entre el almacenamiento *Cloud* y los usuarios del *Cloud*.

5.6.6 Seguridad de las aplicaciones

Un elevado porcentaje de las fugas de datos son el resultado de ataques en la capa de aplicación, particularmente para las aplicaciones web. Por favor revise el Dominio 10 para obtener más información sobre seguridad de las aplicaciones.

5.6.7 Almacenamiento preservador de la privacidad

Casi todos los sistemas de almacenamiento basados en *cloud* requieren de alguna autenticación de los participantes (usuario de *Cloud* y/o CSP²⁶) para establecer relaciones de confianza, ya sea sólo para un punto extremo de la comunicación o para ambos. Aunque los certificados criptográficos pueden ofrecer suficiente seguridad para muchos de estos fines, no suelen cubrir la privacidad, ya que están ligados a la identidad de una persona real (usuario *Cloud*). Cualquier uso de uno de esos certificados muestra la identidad del titular a la parte que solicita la autenticación. Hay muchos escenarios (por ejemplo, el almacenamiento de registros de salud electrónicos) donde el uso de dichos certificados revela innecesariamente la identidad de su titular.

En los últimos 10-15 años, se han desarrollado varias tecnologías para crear sistemas confiables, como certificados criptográficos normales, que al mismo tiempo protegen la privacidad de su titular (es decir, ocultando la identidad del

²⁶ *Cloud Service Provider*, Proveedor de Servicio en *Cloud*

verdadero titular). Dichas credenciales basadas en atributos se emiten como credenciales criptográficas ordinarias (por ejemplo, las credenciales X.509) usando una clave de firma digital (secreta). Sin embargo, las credenciales (ABC) basadas en atributos permiten a su titular transformarlas en una nueva credencial que contiene sólo un subconjunto de los atributos contenidos en la credencial original. No obstante, estas credenciales transformadas pueden ser verificadas igual que las credenciales criptográficas ordinarias (utilizando la clave pública de verificación del emisor) y ofrecen el mismo nivel alto de seguridad.

5.6.8 Digital Rights Management (DRM)

En su núcleo, *Digital Rights Management* cifra el contenido, y entonces aplica una serie de *derechos*. Los derechos pueden ser tan simples como copiar, o tan complejos como especificar restricciones por grupo o usuario en actividades como cortar y pegar, enviar correos, cambiar el contenido, etc. Cualquier aplicación o sistema que trabaja con datos protegidos con DRM debe ser capaz de interpretar e implementar los derechos, lo cual normalmente implica integrarse con un sistema de gestión de claves.

Hay dos categorías en sentido amplio de *Digital Rights Management*:

- **DRM de consumidor** se usa para proteger contenido de amplia distribución como audio, video, y libros electrónicos destinados a audiencias masivas. Hay diversas tecnologías y estándares, y el énfasis está en la distribución unidireccional.
- **DRM corporativo** se usa para proteger el contenido de una organización de forma interna y con sus colaboradores de negocio. El énfasis se pone en derechos más complejos, políticas, e integración con entornos de negocio y particularmente con los servicios de directorio corporativo.

El DRM corporativo puede proteger correctamente el contenido almacenado en *Cloud*, pero requiere una integración profunda de la infraestructura. Es sobre todo útil para la gestión y distribución de contenido basado en documentos. El DRM de consumidor ofrece una buena protección para proteger y distribuir contenido a los clientes, pero no tiene una buena trayectoria dado que, para la mayoría de las tecnologías desarrolladas hasta la fecha, se ha encontrado la forma de romper los mecanismos de protección que aplican.

5.7 Recomendaciones

- Entienda la arquitectura de almacenamiento *Cloud* empleada, lo cual ayudará a determinar el riesgo de seguridad y los controles posibles.
- Elija almacenamiento con dispersión de los datos cuando esté disponible.
- Utilice el ciclo de vida de seguridad de los datos para identificar riesgos de seguridad y determinar los controles más adecuados.
- Monitorice las bases de datos clave internas y los repositorios de archivos con DAM y FAM para identificar grandes migraciones de datos, que podrían indicar que se están migrando datos al *Cloud*.
- Monitorice el acceso de los empleados a Internet con filtrado de URL y/o herramientas DLP para identificar datos delicados que se estén migrando al *Cloud*. Escoja herramientas que incluyan categorías predefinidas para servicios *Cloud*. Considere el uso de filtros para bloquear la actividad no autorizada.

- Cifre todos los datos delicados que se mueven hacia o dentro del *Cloud* en la capa de red, o en los nodos antes de la transmisión por red. Esto incluye todos los servicios y modelos de despliegue.
- Cuando use algún tipo de cifrado de datos, preste especial atención a la gestión de claves (vea el Dominio 11).
- Use el descubrimiento de contenido para escanear el almacenamiento *Cloud* e identificar los datos confidenciales expuestos.
- Cifre volúmenes con información delicada en IaaS para limitar la exposición debida a los *snapshots* o acceso no autorizado por administradores. La técnica específica variará en función de las necesidades operativas.
- Cifre los datos delicados en el almacenamiento de objetos, generalmente con agente cifrado de archivo/carpeta.
- Cifre los datos delicados en las aplicaciones PaaS y el almacenamiento. El cifrado a nivel de aplicación es la opción preferida habitualmente, sobre todo porque pocas bases de datos *Cloud* dispone de cifrado nativo.
- Al utilizar el cifrado de aplicación, las claves deben ser almacenados externamente a la aplicación cuando sea posible.
- Si el cifrado es necesario para SaaS, trate de identificar un proveedor que ofrezca cifrado nativo. Utilice cifrado de proxy si no está disponible y/o se han de asegurar niveles de confianza.
- Utilice DLP para identificar los datos delicados que se estén filtrando de despliegues *Cloud*. Por lo general sólo está disponible para IaaS, y puede no ser viable para todos los proveedores de *Cloud* pública.
- Monitoree las bases de datos con datos delicados con DAM y genere alertas de vulneraciones de política de seguridad. Utilice una herramienta preparada para el *Cloud*.
- Considere un almacenamiento que preserve la privacidad cuando ofrezca infraestructura o aplicaciones en las que el acceso normal pueda revelar información delicada del usuario.
- Recuerde que las brechas más grandes de seguridad son el resultado de una seguridad escasa en las aplicaciones.
- Los proveedores *Cloud* no sólo deben seguir estas prácticas, sino que han de dar visibilidad a sus clientes de las herramientas de seguridad de los datos y las opciones.
- La eliminación o de datos de un proveedor *Cloud*, ya sea debido a la expiración del contrato o cualquier otra razón, se debe cubrir en detalle en la creación del ANS. Esto debe abarcar la eliminación de cuentas de usuario, la migración o la eliminación de datos desde el almacenamiento primario/redundante, entrega de claves, etc.

5.8 Requerimientos

- ✓ Utilice el ciclo de vida de la seguridad de los datos para identificar riesgos de seguridad y determinar los controles más adecuados.
- ✓ Debido a todos los potenciales problemas regulatorios, contractuales y jurisdiccionales de otro tipo, es extremadamente importante entender tanto las ubicaciones lógicas como las físicas de los datos.
- ✓ Monitoree el acceso de los empleados a Internet con filtrado de URL y/o herramientas DLP para identificar datos delicados que migren al *Cloud*.

- ✓ Cifre todos los datos delicados que se mueven hacia o dentro del *Cloud* en la capa de red, o en los nodos antes de la transmisión por red.
- ✓ Cifre los volúmenes con datos delicados en IaaS para limitar la exposición debida a *snapshots* o acceso no autorizado de administradores.
- ✓ Cifre los datos delicados en las aplicaciones PaaS y el almacenamiento.

REFERENCIAS

- [1] RABIN, M. O. 1989. Efficient Dispersal of Information for Security, Load Balancing, and Fault Tolerance. J. ACM, 36(2), 335–348.
- [2] SECUROSIS. 2011. The Data Security Lifecycle. <http://www.securosis.com/blog/data-security-lifecycle-2.0>
- [3] SECUROSIS. 2011. Understanding and Selecting a Data Loss Prevention Solution. <http://www.securosis.com/research/publication/report-data-loss-prevention-whitepaper>
- [4] SECUROSIS. 2008. Understanding and Selecting a Database Activity Monitoring solution. <http://www.securosis.com/research/publication/report-selecting-a-database-activity-monitoring-solution/>
- [5] CHAUM, D. L. Feb. 1981. Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. Communications of the ACM, 24 (2), 84-90.

DOMINIO 6 //

INTEROPERABILIDAD Y PORTABILIDAD

La llegada del *Cloud computing* brinda una escalabilidad sin precedentes a la capacidad de procesado y a la administración de TI de una organización, a diferencia de la que ofrecían las infraestructuras internas tradicionales. La infraestructura *Cloud* permite prácticamente al instante añadir capacidad adicional, moverla o eliminarla según las necesidades de procesado cambiantes de forma dinámica. Se puede iniciar un nuevo sistema de soporte de aplicación para satisfacer la creciente demanda en cuestión de horas en lugar de tardar semanas. Si la demanda desciende, la capacidad adicional puede apagarse con la misma rapidez sin necesidad de hardware extra que ahora estaría sin utilizar. La obtención de beneficios en este entorno más elástico requiere que tanto la Interoperabilidad como la portabilidad sean los objetivos de diseño de cualquier sistema implementado en *cloud*, desde IaaS hasta SaaS.

En un extremo de la balanza, la Interoperabilidad y la Portabilidad permiten escalar un servicio a través de múltiples y dispares proveedores a nivel mundial y que dicho sistema opere y aparezca como un único sistema. En el otro extremo, la Interoperabilidad y la Portabilidad permiten el movimiento sencillo de los datos y las aplicaciones de una plataforma a otra o de un proveedor de servicios a otro.

La Portabilidad y la Interoperabilidad no son cuestiones únicas de los entornos *Cloud* y los aspectos relacionados con su seguridad tampoco son conceptos nuevos introducidos por el *Cloud computing*. Sin embargo, los entornos de procesado abiertos y a menudo compartidos que existen dentro de *Cloud*, hacen que sea necesario tomar precauciones aún mayores que las requeridas para los modelos de procesado tradicionales. *Multi-tenancy* significa que los datos y las aplicaciones residen junto a los datos y aplicaciones de otras empresas y que es posible el acceso a datos confidenciales (intencionadamente o no) a través de plataformas, almacenamiento y redes compartidas.

En esta sección se definen los aspectos críticos que deberían abordarse durante el diseño en cuanto a la Portabilidad y la Interoperabilidad.

Introducción. Las secciones siguientes definen Interoperabilidad y Portabilidad en términos de:

- Introducción a la Interoperabilidad
- Recomendaciones para asegurar la Interoperabilidad
- Una introducción a la Portabilidad
- Recomendaciones para la Portabilidad

6.1 Introducción a la Interoperabilidad

La Interoperabilidad es el requisito necesario para que los componentes de un ecosistema de *Cloud computing* trabajen juntos a fin de alcanzar el resultado deseado. En un ecosistema de *Cloud computing* los componentes pueden proceder de distintas fuentes, tanto *Cloud* como tradicionales, de implementaciones de *Cloud* públicas como privadas (conocidas como *Cloud* híbridas). La Interoperabilidad exige que dichos componentes puedan ser reemplazados por nuevos o distintos componentes de diferentes proveedores de forma transparente, sin que el trabajo se vea afectado, como también debería poder realizarse el intercambio de datos entre sistemas.

Las empresas, con el tiempo, tomarán decisiones que les llevarán a cambiar de proveedor. Las razones para buscar un cambio son:

- Un aumento inaceptable del coste en el momento de renovación del contrato.
- La posibilidad de obtener el mismo servicio a un precio más económico.
- El cese de la actividad del proveedor.
- El proveedor cierra de repente uno o más de los servicios que se estaban utilizando sin un plan de migración aceptable.
- Una reducción inaceptable de la calidad del servicio, como la incapacidad para alcanzar los requisitos clave de rendimiento o el incumplimiento con los contratos de nivel de servicio (**ANS**)
- Una disputa comercial entre el cliente de *Cloud* y el proveedor.

La falta de Interoperabilidad (y también de Portabilidad) puede conducir al cliente a verse limitado a trabajar con un proveedor de servicios de *Cloud* concreto.

Cuando se plantea un proyecto de *Cloud*, el grado en que la Interoperabilidad puede alcanzarse o mantenerse, a menudo depende de la medida en que un proveedor de *Cloud* utilice arquitecturas abiertas o publicadas y protocolos estándar, así como **API** estándar. Sin embargo, muchos proveedores de estructuras de *Cloud* "abiertas" y "basadas en estándares" proporcionan *hooks* propietarios y extensiones (por ejemplo, Eucalyptus) y mejoras que pueden obstaculizar tanto la Interoperabilidad como la Portabilidad.

6.2 Una Introducción a la Portabilidad

La Portabilidad define la facilidad con la que los componentes de aplicación se migran y son reutilizados en otros lugares independientemente del proveedor, la plataforma, el sistema operativo, la infraestructura, la ubicación, el tipo de almacenamiento, el formato de los datos o las API.

Deben tenerse en cuenta la Portabilidad y la Interoperabilidad tanto si la migración de *cloud* se realiza a soluciones de implementaciones públicas o privadas, como a *Cloud* híbridas. Se trata de elementos importantes a tener en cuenta para la selección del modelo de servicio, independientemente de si la estrategia de migración es SaaS, PaaS o IaaS.

La Portabilidad es un aspecto clave a tener en cuenta a la hora de seleccionar los proveedores de *Cloud*, ya que puede ayudar a prevenir la dependencia de un único proveedor y a distribuir los beneficios del negocio permitiendo que se den casos de uso de *Cloud* idénticos a través de soluciones de diferentes proveedores de *Cloud*, ya sea para fines de recuperación de desastres o para el despliegue global de una única solución distribuida.

Lograr la Portabilidad para un servicio de *Cloud* generalmente depende de los dos servicios que operan en el mismo octante arquitectónico del Cubo *Cloud*, tal como se define en el Dominio Uno. Cuando los servicios operan en octantes diferentes del *Jericho Cube* (Figura 4), por lo general, el paso entre servicios implica la migración previa al servicio interno de nuevo, antes de volver a externalizarlo a un servicio de *Cloud* alternativo.

Si no se abordan adecuadamente la Portabilidad y la Interoperabilidad en una migración de *Cloud*, podrían no alcanzarse los beneficios esperados con el paso a *Cloud*, derivando en costosos problemas o retrasos del proyecto como consecuencia de determinados factores que deberían evitarse, tales como:

- Dependencia de una única aplicación, vendedor o proveedor – la elección de una solución de *Cloud* en particular puede restringir la capacidad de cambiar a otra oferta de *Cloud* o a otro proveedor.
- Incompatibilidad de capacidades de procesamiento y conflictos que causan la interrupción del servicio – las diferencias entre proveedores, plataformas o aplicaciones pueden conllevar incompatibilidades que hagan que las aplicaciones no funcionen correctamente dentro de una infraestructura de *Cloud* distinta.
- Un cambio inesperado en el proceso de negocio o una reingeniería de la aplicación – el paso a un nuevo proveedor de *Cloud* puede implicar la necesidad de rediseñar cómo funciona un proceso o requerir cambios de código para mantener el comportamiento original.
- Migración o conversión de datos costosa – la falta de formatos de Interoperabilidad y Portabilidad puede dar lugar a cambios no deseados en los datos al pasar a un nuevo proveedor.
- Reciclaje o actualización de una nueva aplicación o software de gestión.
- Pérdida de datos o seguridad de la aplicación – diferentes políticas y controles de seguridad, gestión de claves o protección de datos entre los distintos proveedores pueden abrir brechas de seguridad ocultas al pasar a un nuevo proveedor o plataforma.

La migración de servicios a *Cloud* es una forma de externalización; la regla de oro de la externalización es "entender el contrato por adelantado y planear cómo salir de él". La Portabilidad (y hasta cierto punto la Interoperabilidad), debería ser un criterio clave en la estrategia de cualquier organización para pasar a servicios en *Cloud*, a fin de desarrollar una estrategia de salida viable.

6.3 Recomendaciones

6.3.1 Recomendaciones para la Interoperabilidad

Hardware –Hardware de Computadora Física

Inevitablemente, el hardware cambiará con el tiempo y de un proveedor a otro, dejando brechas de Interoperabilidad si se requiere acceso directo al hardware.

- Siempre que sea posible, conviene utilizar la virtualización para eliminar muchos de los aspectos a valorar a nivel de hardware, recordando que la virtualización no implica necesariamente la eliminación todos los aspectos relacionados con el hardware, especialmente en los sistemas actuales.
- Si es necesario acceder directamente al hardware, al pasar de un proveedor a otro es importante asegurarse que existen los mismos o mejores controles de seguridad física y administrativa.

Dispositivos de Red Físicos

Los dispositivos de red, incluyendo dispositivos de seguridad, serán diferentes según el proveedor de servicios, como también lo serán las API y el proceso de configuración.

- Para mantener la Interoperabilidad, la abstracción del hardware físico de la red y la seguridad, debería trabajarse en un dominio virtual. En la medida de lo posible, debería aplicarse lo mismo para las API.

Virtualización

Mientras que la virtualización puede ayudar a disipar las preocupaciones relacionadas con el hardware físico, existen claras diferencias entre los hipervisores comunes (tales como ZEN, VMware entre otros).

- Utilizar formatos abiertos de virtualización como OVF para ayudar a garantizar la Interoperabilidad.
- Documentar y comprender qué *hooks* de virtualización específicos se utilizan sin importar el formato. Puede que aún no trabaje sobre otro hipervisor.

Marcos de referencia

Los diferentes proveedores de plataformas ofrecen distintos marcos de referencia para aplicaciones *Cloud* y existen diferencias entre ambos que afectan a la Interoperabilidad.

- Investigar las APIs para determinar dónde se encuentran las diferencias y planificar los cambios necesarios que se requieran para la capacidad de procesamiento de aplicaciones al pasar a un nuevo proveedor.
- Utilizar APIs abiertas y publicadas para asegurar la mayor Interoperabilidad entre los componentes y para facilitar la migración de aplicaciones y datos si se hiciese necesario cambiar de proveedor de servicios.
- Las aplicaciones en *Cloud* a menudo interoperan a través de Internet y los cortes se pueden anticipar. Determinar cómo un fallo en un componente (o una respuesta lenta) afectará a los demás componentes, y evitar dependencias del estado de las conexiones que pongan en riesgo la integridad de los datos del sistema cuando falla un componente remoto.

Almacenamiento

Los requisitos de almacenamiento variarán según los tipos de datos. Los datos estructurados a menudo requieren un sistema de base de datos o formatos específicos de la aplicación. Los datos no estructurados normalmente siguen cualquier tipo de formato de las aplicaciones comunes que utilizan los procesadores de texto, hojas de cálculo y gestores de presentación. Aquí, el aspecto a valorar debería centrarse en poder mover los datos almacenados de un tipo de servicio a otro sin problemas.

- Almacenar los datos no estructurados en un formato establecido que facilite su portabilidad.
- Evaluar la necesidad de cifrado de los datos en tránsito.
- Revisar los sistemas de bases de datos compatibles y evaluar los requisitos de conversión si es necesario.

Seguridad

Los datos y las aplicaciones en *Cloud* residen en sistemas de los que el usuario no es propietario y es probable que sólo tenga un control limitado sobre ellos. Deben tenerse en cuenta una serie de puntos importantes para la seguridad en la Interoperabilidad:

- Utilizar SAML o WS-Security para la autenticación de modo que los controles puedan ser interoperables con otros sistemas basados en estándares. Véase el Dominio 12 para más información.
- Cifrar los datos antes de subirlos a *Cloud* asegurará que no se pueda acceder a ellos indebidamente dentro de los entornos *Cloud*. Véase el Dominio 11 para más detalles sobre el cifrado.
- Cuando se están utilizando claves de cifrado, investigar cómo y dónde se almacenan las claves para garantizar que el acceso a los datos cifrados existentes está restringido. Véase el Dominio 11 para obtener más detalles sobre la gestión de claves.
- Comprender las responsabilidades y obligaciones en caso de que se comprometa la seguridad debido a brechas imprevistas en los métodos de protección ofrecidos por el proveedor de servicios.
- La información de ficheros de log debería ser manejada con el mismo nivel de seguridad que todos los demás datos que se suben a *Cloud*. Asegúrese de que los archivos de logs son interoperables para garantizar que permanecen inalterados y que es posible analizarlos antes y después de subirlos, así como también que sean compatibles con cualquier sistema de administración de logs que esté en uso.
- Al completar una subida, asegurar que todos los datos, registros y demás información se eliminan del sistema original.

6.3.2 Recomendaciones de portabilidad

Hay una serie de cuestiones pendientes en el proceso de la migración a *cloud*. Las consideraciones de Portabilidad y las recomendaciones que impactan en dicho proceso incluyen:

- **Nivel de servicio.** Los ANS dependerán de los proveedores, por lo tanto, es necesario entender cómo podría afectar esto a la capacidad para cambiar de proveedor.
- **Arquitecturas diferentes.** Los sistemas en *Cloud* pueden residir en plataformas con distintas arquitecturas. Es importante ser consciente de que esto limitará la Portabilidad, por lo que resulta necesario entender las dependencias entre el servicio y la plataforma que incluirá API, herramientas, la lógica de la aplicación y otras restricciones.
- **Integración de la seguridad.** Los sistemas *Cloud* conllevan aspectos a valorar específicos en la portabilidad para mantener la seguridad, incluyendo:
 - Los mecanismos de autenticación e identificación para el acceso de usuarios o procesos a los sistemas ahora tienen que aplicarse a lo largo de todos los componentes del sistema *cloud*. La utilización de estándares abiertos para la gestión de identidades, como SAML, ayudará a asegurar la Portabilidad. Desarrollar un sistema IAM

interno para apoyar las afirmaciones de SAML y el sistema interno para aceptar SAML, ayudará a la futura Portabilidad del sistema a *Cloud*.

- Las claves de cifrado deben ser custodiadas a nivel local y, cuando sea posible, mantenidas localmente.
- Los metadatos son un aspecto de la información digital que a menudo se pasa por alto y que, normalmente, no es visible directamente cuando se trabaja con archivos o documentos. Los metadatos se convierten en un factor importante en *Cloud* porque se mueven con los documentos. Cuando se pasan archivos y sus metadatos a un nuevo entorno de *Cloud*, hay que asegurarse de que las copias de los metadatos del archivo se han eliminado de forma segura para impedir que queden disponibles y la información sea comprometida.

6.3.3 Recomendaciones para los distintos modelos de *cloud*

Existen una serie de riesgos genéricos y recomendaciones que son comunes a todos los modelos de *cloud*:

- Al sustituir a los proveedores de *cloud* es normal que haya resistencia por parte de dicho proveedor. Esto debe estar recogido en el contrato, como se indica en el Dominio 3, en el Programa de Continuidad de Negocio, como se indica en el Dominio 7, y como parte del Gobierno global en el Dominio 2.
- Entender el tamaño de los datos alojados en un proveedor de *Cloud*. El tamaño de los datos puede causar una interrupción del servicio durante una transición o un periodo de transición más largo de lo previsto. Muchos clientes han encontrado que el uso de un proveedor de mensajería para enviar los discos duros es más rápido que la transmisión electrónica de una gran cantidad de datos.
- Es necesario documentar la arquitectura de seguridad y la configuración de los controles individuales de seguridad de los componentes para que se puedan soportar las auditorías internas, así como para facilitar la migración a los nuevos proveedores y ayudar con la validación del nuevo entorno.

Infrastructure as a Service (IaaS)

Cuando la responsabilidad del proveedor de *Cloud* es proporcionar servicios básicos de computación como almacenamiento, energía, etc., el cliente de *Cloud* es responsable de la mayor parte del diseño de tareas relacionadas con la Interoperabilidad. El proveedor de *Cloud* debería proporcionar hardware estandarizable y recursos informáticos que puedan interactuar con varios sistemas dispares con el mínimo esfuerzo. El proveedor de *Cloud* debe seguir estrictamente los estándares de la industria para mantener la Interoperabilidad. El proveedor debería ser capaz de soportar situaciones complejas como una intermediación en *Cloud* (*Cloud brokerage*), ráfagas de *Cloud*, *Cloud* híbridas, asociaciones *multi-cloud*, etc.

- Entender como las imágenes de las máquinas virtuales pueden ser capturadas y trasladadas a nuevos proveedores de *Cloud* que usan diferentes tecnologías de virtualización. Por ejemplo *Distributed Management Task Force (DMTF) Open Virtualization Format (OVF)*.
- Identificar o eliminar (o al menos documentar) las extensiones específicas del entorno de máquina virtual de cualquier proveedor.
- Entender las prácticas que se han establecido para asegurar que el desaprovechamiento de las imágenes de la máquina virtual se realiza después de que la aplicación ha sido portada desde el proveedor de *Cloud*.

- Entender las prácticas utilizadas para la destrucción de los discos y de los dispositivos de almacenamiento.
- Entender las dependencias de hardware/plataformas basadas en la necesidad de ser identificadas antes de la migración de la aplicación y los datos.
- Solicitar el acceso a los logs del sistema, trazas y acceso a los registros de facturación del proveedor de *Cloud* preexistente.
- Identificar las opciones para reanudar o ampliar el servicio con el proveedor de *Cloud* preexistente en parte o en su totalidad si el nuevo servicio resulta ser inferior.
- Determinar si hay funciones de nivel de gestión, interfaces o APIs que son incompatibles o no las implementa el nuevo proveedor.
- Entender los costes involucrados en la transferencia de datos hacia y desde un proveedor de *Cloud*.
- Determinar qué medios se soportan para mover datos tan eficientemente como sea posible a *Cloud* utilizando capacidades estándar como puede ser la compresión de datos.
- Entender qué seguridad se proporciona y quién mantiene el acceso a las claves de cifrado.

Platform as a Service (PaaS)

El proveedor de *Cloud* es responsable de proporcionar una plataforma en la que los usuarios puedan construir sus sistemas. Se proporcionará un entorno de ejecución y un conjunto de aplicaciones integradas. Esto permite a los desarrolladores crear y desplegar rápidamente las aplicaciones de usuario en las plataformas ofertadas sin necesidad de construir la infraestructura. El proveedor de *Cloud* proporcionará la infraestructura completa y su mantenimiento a los usuarios.

- Cuando sea posible, se utilizarán los componentes de la plataforma con una sintaxis estándar, API y estándares abiertos, por ejemplo, *Open Cloud Computing Interface (OCCI)*²⁷
- Entender qué herramientas están disponibles para la transferencia segura de datos, backup y restauración.
- Entender y documentar los componentes de la aplicación y los módulos específicos del proveedor de PaaS y desarrollar una arquitectura de aplicación con capas de abstracción para minimizar el acceso directo a módulos propietarios.
- Entender cómo los servicios básicos, como la monitorización, el registro y la auditoría, se transferirán a un nuevo fabricante.
- Entender la protección existente para los datos ubicados en *Cloud* y para los datos generados y mantenidos en *Cloud*.
- Entender las funciones de control proporcionadas por el antiguo proveedor de *Cloud* y cómo se traducen al nuevo proveedor.

²⁷ OCCI - Open Cloud Computing Interface (Interfaz de *Cloud Computing* abierto)

- Al migrar a una nueva plataforma, entender el impacto en el rendimiento y la disponibilidad de la aplicación y cómo se medirá este impacto.
- Entender cómo las pruebas se completarán antes y después de la migración para verificar que los servicios o aplicaciones funcionan correctamente. Asegurar que las responsabilidades para las pruebas tanto del usuario como del proveedor son conocidas y están bien documentadas.

Software as a Service (SaaS)

El proveedor de *Cloud* proporciona las capacidades de aplicación a través de *Cloud* y el cliente sólo gestiona sus operaciones y la información que entra y sale del sistema. El cliente necesita un navegador y la mayor parte de las tareas administrativas a todos los niveles recaen en el proveedor.

- Realizar regularmente extracciones de datos y backups a un formato que se pueda utilizar independientemente del proveedor de SaaS.
- Entender si los metadatos se pueden conservar y migrar.
- Si es necesario, utilizar servicios de custodia de datos.
- Entender que cualquier herramienta personalizada tendrá que ser rediseñada o el nuevo proveedor tendrá que proporcionar y mantener estas herramientas.
- Revisar y auditar para asegurar la consistencia de la efectividad de los controles tanto para los nuevos como para los antiguos proveedores.
- Asegurar que pueden ser migrados los backups y otras copias de logs, los registros de acceso y cualquier otra información pertinente que pueda ser solicitada para el cumplimiento legal.
- Entender las interfaces de gestión, de monitorización y de informes y su integración entre varios entornos.
- Probar y evaluar todas las aplicaciones antes de su migración y realizar una ejecución en paralelo, si es posible, antes de dicha migración.

Cloud Privado

El *Cloud* privado es aquel en el que el usuario ejecuta un entorno/servicio de *Cloud* dentro de su empresa o utiliza *Cloud* privado del proveedor (normalmente es una ampliación de la red interna dentro de un centro de alojamiento de un proveedor de servicios).

- Asegurar la interoperabilidad que existe entre los hipervisores comunes como KVM, VMware, Xen.
- Asegurar que las APIs estándar se utilizan para gestionar funciones como usuarios y la gestión de sus privilegios, gestión de las imágenes de las máquinas virtuales, gestión de las máquinas virtuales, gestión de redes virtuales, gestión de servicios, gestión del almacenamiento, gestión de la infraestructura, gestión de la información, etc.

Cloud Público

La Interoperabilidad en *Clouds* públicos conlleva una mayor exposición a los interfaces de *Cloud*. Pueden ser fabricantes específicos o especificaciones públicas e interfaces como OCCl, **libcloud**, etc.

- Asegurar que los proveedores de *Cloud* exponen interfaces comunes y/o abiertas para acceder a todas las funciones del servicio que ofrecen en *Cloud*.

Cloud Híbrida

En este escenario, la infraestructura privada local del usuario debería ser capaz de trabajar con los proveedores de *Cloud* externos. Un escenario común es el de la proliferación de *Clouds* donde una empresa comparte la carga con proveedores de *Cloud* externos para satisfacer los picos de demanda.

- Asegurar que los proveedores de *Cloud* ofrecen interfaces abiertas para acceder a todas las funciones de *Cloud* de su oferta de servicios.
- Asegurar la capacidad para establecer relaciones con varios proveedores de *Cloud* para permitir mayores niveles de escalabilidad.

REFERENCIAS

- [1] <http://msdn.microsoft.com/en-us/library/cc836393.aspx>
- [2] <http://blogs.msdn.com/b/eugenioip/archive/2010/01/12/adfs-wif-on-amazon-ec2.aspx>
- [3] <http://download.microsoft.com/download/6/C/2/6C2DBA25-C4D3-474B-8977-E7D296FBFE71/EC2-Windows%20SSO%20v1%20--Chappell.pdf>
- [4] <http://www.zimbio.com/SC+Magazine/articles/6P3njtcljmR/Federation+2+0+identity+ecosystem>
- [5] <http://www.datacenterknowledge.com/archives/2009/07/27/cloud-brokers-the-next-big-opportunity/>
- [6] http://blogs.oracle.com/identity/entry/cloud_computing_identity_and_access
- [7] http://www.opengroup.org/jericho/cloud_cube_model_v1.0.pdf
- [8] <http://www.burtongroup.com>
- [9] <http://www.pkware.com/appnote>
- [10] <http://www.apps.ietf.org/rfc/rfc4880.html>



SECTION III //
OPERACIONES EN
ENTORNO *CLOUD*

DOMINIO 7 //

SEGURIDAD TRADICIONAL, CONTINUIDAD DE NEGOCIO Y RECUPERACIÓN DE DESASTRES

Los aspectos de seguridad inherentes al modelo de alojamiento han asumido una gran importancia y criticidad, debido al carácter emergente del *Cloud computing* como tecnología preferida para la externalización de operaciones de IT. Adicionalmente, los riesgos asociados a encomendar información confidencial y sensible a terceros o a proveedores dedicados de servicios de *Cloud* (CSP) son inherentes al concepto de *Cloud computing*.

La evolución de los servicios de *Cloud* ha facilitado a las organizaciones la realización de más con menos: menos recursos y mejor eficiencia operativa, lo que aporta numerosos beneficios tangibles al negocio. Sin embargo, existen riesgos de seguridad inherentes que deben ser evaluados, gestionados y resueltos antes de que las organizaciones tengan confianza en la externalización segura de sus requerimientos de IT a los proveedores de servicios de *Cloud*.

Uno de los objetivos de este dominio es el de aportar a los CSP un entendimiento común de la seguridad tradicional (seguridad física) en los servicios de *Cloud*. La seguridad tradicional puede ser definida como las medidas tomadas para garantizar la seguridad de la información, personal y material contra robo, espionaje, sabotaje u otros daños. En el contexto específico de *Cloud*, la seguridad tradicional incluye la protección de la información, productos y personas.

Esta sección mapea con los dominios IS-01 e IS-02 de la Matriz de Control Cloud, así como con el Dominio 9 de la ISO/IEC27002.

Una adecuada seguridad de la información despliega muchas capas diferenciadas para lograr su objetivo, lo que se denomina seguridad en capas o defensa en profundidad. A la hora de implementar medidas de seguridad, es importante ser consciente de que ninguna medida es cien por cien segura. Por tanto, la seguridad de la información utiliza varias capas de profundidad para lograr un nivel de seguridad combinado. La existencia de debilidades en alguna de estas capas puede originar una brecha de seguridad. La protección física es el paso inicial en un enfoque por capas para la gestión de la seguridad de la información en *Cloud*. Si es inexistente, se implementa incorrectamente, es débil, se ejecuta de manera inconsistente, se trata como un proyecto (*fire-n-forget*), o no se mantiene y revisa apropiadamente, ni las mejores medidas de seguridad lógica cubrirán las debilidades en seguridad física, y por tanto la seguridad general puede fallar.

Un programa tradicional efectivo de seguridad está formado por un conjunto de análisis de riesgos, análisis de vulnerabilidades, políticas de BCP/DR, y procesos y procedimientos, que han sido desarrollados adecuadamente y que son revisados y probados de forma periódica. Los programas de seguridad física desarrollados adecuadamente desembocarán en una seguridad física que, a lo largo del tiempo, resulta escalable al negocio, repetible a lo largo de la organización, medible, sostenible, defendible, de mejora continua y rentable.

Introducción: Algunos de los riesgos de seguridad asociados al *Cloud computing* son únicos y es en este contexto en el que los proveedores de servicios de *Cloud* deben valorar la continuidad del negocio, la recuperación ante desastres y los entornos de seguridad tradicional (i.e. usando estándares y mejores prácticas internacionales como **TOGAF**²⁸, **SABSA**²⁹, **ITIL**³⁰, **COSO**³¹, o **COBIT**³²). Este dominio valora:

- El establecimiento de una Función de Seguridad Física
- La Seguridad Física de Recursos Humanos
- La Continuidad de Negocio
- La Recuperación ante Desastres

Esta sección mapea con los dominios FS-01, FS-02, FS-03 y FS-04 de la Matriz de Control Cloud, así como con el Dominio 9 de la ISO/IEC27002.

7.1 Estableciendo una Función de Seguridad Tradicional

Muchas organizaciones no han prestado suficiente atención a la posible obsolescencia en materia de seguridad de equipamiento IT o a la tecnología de red. Esto ha originado que en muchas organizaciones la instalación física de equipamiento informático, redes y sistemas de comunicaciones no cuente con adecuados emplazamientos físicos diseñados que permitan proteger los activos y mantener la disponibilidad.

Para establecer una adecuada seguridad física para el equipamiento de IT, tecnologías de red y activos de telecomunicaciones en un entorno *Cloud*, es importante que las responsabilidades sean asignadas a personal apropiado dentro del proveedor de *Cloud*. Un individuo de la dirección del proveedor de *cloud* es responsable de gestionar la planificación, implementación y mantenimiento de los planes y procedimientos relevantes. Adicionalmente, es necesario tanto formar como evaluar al personal responsable de la seguridad física. A la hora de establecer una función de seguridad física en un entorno *Cloud*, se deben considerar los siguientes aspectos:

- Las necesidades de seguridad del equipamiento y servicios que están siendo protegidos.
- Los recursos humanos disponibles para seguridad física.
- La gestión de las iniciativas de seguridad física así como los recursos disponibles previos a la migración a *Cloud*.
- Recursos financieros disponibles en dichas iniciativas

La seguridad física puede ser tan simple como añadir una puerta con cerradura o tan elaborada como implementar múltiples capas de barreras y guardias de seguridad armados. Una seguridad física adecuada se basa en la defensa en capas que, combinadas apropiadamente, permiten gestionar el riesgo mediante la disuasión y dilación de las amenazas a la seguridad física. Sin embargo, las amenazas físicas a la infraestructura, personal y sistemas no están limitadas a las posibles intrusiones. Para mitigar estos riesgos, se despliega una combinación de defensas tanto pasivas como activas, en la que se incluyen medidas tales como:

- Obstáculos para disuadir y retrasar eventos, incidentes y ataques.

²⁸ **TOGAF** - The Open Group Architecture Framework

²⁹ **SABSA** - Sherwood Applied Business Security Architecture

³⁰ **ITIL** - Information Technology Infrastructure Library

³¹ **COSO** - Committee of Sponsoring Organizations

³² **COBIT** - Control Objectives for Information and Related Technology

- Sistemas de detección para monitorizar las condiciones medioambientales y de seguridad.
- Un protocolo de respuesta antes incidentes diseñado para repeler, aprehender o desanimar a los atacantes.

Adicionalmente, la seguridad física se aborda desde diversas perspectivas tanto en diseño como en implementación:

- Diseño medidas medioambientales.
- Mecánico, electrónico y procedimientos de control.
- Detección, respuesta y procedimientos de recuperación.
- Identificación, autenticación, autorización y control de acceso del personal.
- Políticas y procedimientos, incluyendo la formación del personal.

7.1.1 Evaluación de la Seguridad Física Tradicional

Al evaluar la seguridad tradicional de un CSP, los clientes deben considerar los aspectos de la infraestructura como servicio (IaaS), incluyendo la propia del centro de procesamiento de datos (CPD) del proveedor. Esto incluye tanto la ubicación física de las instalaciones, como la documentación de riesgos críticos y factores críticos de recuperación.

7.1.1.1 Ubicación física de las instalaciones del CSP

Para una organización que depende de un servicio de *Cloud*, es importante entender de la infraestructura de *Cloud* de la que depende. Por tanto, uno de los aspectos que debería llevar a cabo es una evaluación crítica de la ubicación física del CPD.

A continuación se listan algunas sugerencias para evaluar la localización física de las instalaciones:

- Comprobar si la localización de la infraestructura se encuentra en una zona de actividad sísmica e identificar los riesgos de actividad sísmica.
- Las instalaciones no deberían estar ubicadas en una región geográfica con riesgo de: inundaciones, desplazamiento de tierra u otros desastres naturales.
- Las instalaciones no deberían estar en un área de alta criminalidad, o de alta agitación política o social.
- Comprobar la accesibilidad de la ubicación de las instalaciones (y la frecuencia de inaccesibilidad).

7.1.1.2 Revisión documental

La documentación que soporta las operaciones de recuperación ante desastres es crítica a la hora de evaluar la preparación de la compañía de alojamiento TI para la recuperación ante una catástrofe. Por tanto, antes de la contratación de un proveedor de alojamiento se debería revisar la siguiente documentación:

- Análisis de riesgos.
- Valoración de riesgos.

- Valoración de vulnerabilidades.
- Plan de continuidad de negocio.
- Plan de recuperación de desastres.
- Políticas de seguridad física y ambiental.
- Procedimientos de baja de cuentas de usuario.
- Plan de contingencia, incluyendo protocolos de test.
- Plan de reporte y respuesta ante incidentes, incluyendo protocolos de test.
- Plan de respuesta de emergencia.
- Diseño de las instalaciones – salidas de emergencia, situación de las cámaras del CCTV, puntos seguros de entrada.
- Plan de evacuación y directrices en caso de incendio.
- Plan de evacuación y procedimientos en caso de emergencia.
- Procedimientos de comunicación en caso de crisis.
- Números de contacto de emergencia.
- Revisión de los accesos de los usuarios a las instalaciones / Registros de auditoría.
- Formación en materia de concienciación de la seguridad: documentación, presentaciones, folletos, etc.
- Registros de asistencia a la formación de concienciación de la seguridad.
- Plan de sucesión para ejecutivos clave.
- Documentación técnica – planos del cableado eléctrico, sistemas de gestión y control de los edificios, sistemas de alimentación ininterrumpida, aire acondicionado.
- Calendario de mantenimiento de los sistemas eléctricos, generadores y CCTV.
- Contratos de los proveedores del servicio de gasoil de emergencia.
- Listado del personal autorizado a acceder a las instalaciones.
- Perfiles del equipo de Seguridad, incluyendo su biografía y antecedentes.
- Informes acerca del nivel de experiencia del equipo de Seguridad (que deberían ser realizados al menos anualmente).
- Contratos de mantenimiento anual para equipamiento y dispositivos clave (priorizando los **ANS** relacionados con el tiempo de inactividad y de restauración de equipamiento y dispositivos).

Hay áreas críticas de la documentación en las cuales el contratante de un servicio de *Cloud* debería focalizar su revisión, con el fin de asegurarse de que sus riesgos están mitigados. Las siguientes recomendaciones pueden ser críticas para garantizar los intereses de un futuro cliente de *cloud* cuando realice la transición a *Cloud*:

- Comprobar si todos los documentos están vigentes y actualizados. Estos documentos deben ser revisados por el CSP al menos una vez al año. La fecha de revisión y la firma por parte de la Dirección deben ser incluidas y validadas como evidencia de la revisión interna.
- Aquellas políticas y procedimientos que deben ser accesibles para los empleados, deben estar disponibles a través de una Intranet a la cual los empleados del CSP puedan acceder en cualquier momento. El equipo de seguridad debe tener especial cuidado para asegurarse que los documentos de la Intranet son la última versión, debidamente aprobados por la Dirección.
- Todos los procedimientos y políticas serán efectivos solamente cuando los empleados sean conscientes de ellos. Para comprobarlo, se debe verificar si el CSP cuenta con un programa de concienciación de seguridad. El CSP debería asegurarse que los empleados reciben formación adecuada en materia de concienciación de seguridad como mínimo una vez al año, disponiendo de registros de asistencia firmados. Además, los nuevos empleados que se incorporen a la organización deberán asistir a una sesión de orientación en seguridad como parte del programa de introducción a la compañía, en la cual se deberán cubrir las políticas y procedimientos clave, y se deberá disponer de registros de asistencia firmados y disponibles para su revisión en cualquier momento. Adicionalmente, para lograr que las sesiones sea efectivas, deberían estar lideradas por personal experimentado del equipo de seguridad.

7.1.1.3 Cumplimiento con los Estándares Internacionales y por Industria de Seguridad

Se debe garantizar que el CSP cumple con estándares globales de seguridad como la ISO27001 ISMS u otros estándares de la industria como TOGAR, SABSA, ITIL, COSO o COBIT. Estos estándares son inestimables a la hora de evaluar el nivel de seguridad y el grado de madurez del CSP.

- Verificar el certificado de cumplimiento y su validez.
- Buscar evidencias verificables de la asignación de recursos, tales como presupuestos y personal que sustenten el programa de cumplimiento.
- Verificar los informes de auditoría interna y obtener evidencia de las acciones correctoras llevadas a cabo sobre las deficiencias.

7.1.1.4 Inspección visual de las instalaciones del CSP

Alcance

Se debe evaluar el Perímetro de Seguridad del Centro de Procesamiento de Datos a la hora de determinar qué áreas requieren cobertura física. A continuación se enumeran áreas de alto riesgo que deben ser aseguradas:

- Áreas administrativas.
- Recepción.
- Aparcamiento.

- Almacén.
- Salidas de emergencia.
- Centro de control del CCTV.
- Centro de control del Aire Acondicionado (AHU).
- Vestuarios
- Centro de control del Sistema de Alimentación Ininterrumpida (UPS).
- Sala del generador.
- Tanques de almacenamiento de gasoil.

Señalización

Se deben buscar las siguientes indicaciones, que deben estar desplegadas de forma prominente en los lugares apropiados de las instalaciones:

- Mapa de las rutas de escape en caso de incendio y salidas de emergencia.
- Directrices en caso de incendio.
- Señalización de seguridad anti incendios
- Cartelería e instrucciones de seguridad.
- Posters explicativos con medidas para evitar que personal no autorizado acceda, por ejemplo empleando técnicas de ingeniería social
- Información relativa a temperatura / humedad.
- Señalización de las áreas de peligro.
- Número de los contactos de emergencia.
- Diagrama de escalado de emergencias.

7.1.2 Infraestructura de Seguridad

El perímetro de seguridad es importante ya que sirve como primera línea de protección contra intrusos y visitantes indeseados. Los principios asociados al perímetro de seguridad han experimentado un cambio radical con los avances tecnológicos. Las cuatro Ds del perímetro de seguridad son *Deter, Detect, Delay* and *Deny* (Disuadir, Detectar, Retrasar y Denegar) a los intrusos que pretendan acceder a las instalaciones.

Las siguientes cualidades son aspectos claves a la hora de seleccionar un proveedor de infraestructura de seguridad. Dependiendo del diseño y de la función del proveedor de servicios de *Cloud*, la siguiente lista debe ser analizada y monitorizada durante el proceso de selección. Se debe tener especial cuidado a la hora de asegurar que la

infraestructura física es adecuada al tamaño, naturaleza y volumen de las operaciones que se realizan en las instalaciones. Los controles de seguridad deben estar posicionados estratégicamente y con unos niveles de calidad acorde a estándares reconocidos y mejores prácticas.

- Asegurar los Puntos de Entrada – Sistemas de control de acceso (tarjetas de proximidad / sistemas biométricos).
- Sistemas de Control de Acceso conectados al panel de control de incendios para emergencias.
- Sistemas de detección de movimiento, sistemas de detección de calor, detectores de rotura de cristal.
- Equipamiento de seguridad anti incendios – tuberías de agua a presión, tomas de agua, mangueras, detectores de humo y aspersores.
- Extintores.
- Salidas anti incendios (no deben estar cerradas o bloqueadas).
- Barras de pánico en las puertas anti incendios.
- Sirenas y luces de alarma.
- Circuito cerrado de TV y servidor de grabación de video (DVR), incluyendo planificación de copias de seguridad.
- Cierres y alarmas de efecto retardado en las puertas.
- Sistemas de supresión de incendios de gas en los CPDs.
- Destructoras de papel cerca de las impresoras.
- Desmagnetizador de dispositivos o sistemas de destrucción segura de discos.
- Kit del Equipo de Respuesta de Emergencia (ERT Kit).
- Auriculares walkier-talkie para el personal de seguridad.
- Alarmas anti coacción bajo la mesa de seguridad y en posiciones estratégicas (ocultas).
- Detectores de metales portátiles y de marco (si son necesarios).
- Dispositivos resistentes al fuego para el almacenamiento de documentos/dispositivos.

7.2 Seguridad Física de los Recursos Humanos

El propósito del control físico de recursos humanos es minimizar el riesgo de que el personal del propio proveedor de *Cloud* comprometa las operaciones y el servicio prestado. Por ejemplo, un usuario con conocimientos y acceso físico a la consola, puede superar la mayor parte de las medidas proactivas de seguridad lógica simplemente

Esta sección mapea con los dominios IS-15, FS-05, FS-06, FS-07 y FS-08 de la Matriz de Control Cloud, así como con el Dominio 9 de la ISO/IEC27002.

apagando el sistema o accediendo con un usuario *root* o de administración. Adicionalmente, un armario de cableado puede proporcionar acceso oculto a la red o un medio para sabotear las redes existentes. Por tanto, se deben considerar las siguientes medidas:

- Roles y responsabilidades (i.e. a través de una matriz estilo RACI³³).
- Verificación de antecedentes.
- Acuerdos con los empleados (i.e. Acuerdos de Confidencialidad).
- Proceso de baja de empleados.
- Concienciación y formación de políticas corporativas (i.e. Código de conducta o Negocio).

Los roles y responsabilidades son parte del entorno *Cloud*, en el cual personas y procesos, junto con la tecnología, se integran para mantener la seguridad del proveedor de una forma consistente. La segregación de funciones requiere al menos dos personas con diferentes responsabilidades para completar una transacción o proceso de extremo a extremo. Es esencial, para proteger a los usuarios del *Cloud*, evitar los conflictos de intereses. Por tanto, se deben implementar medidas destinadas a evitar y monitorizar este riesgo. La segregación de funciones proviene originariamente de la contabilidad y la gestión financiera, pero sus beneficios permiten cubrir otras necesidades de mitigación de riesgo, por ejemplo, relacionadas con la seguridad física, disponibilidad y protección de sistemas.

La segregación de funciones se implementa a través de la eliminación de aquellas combinaciones de roles de alto riesgo (por ejemplo, no disponiendo de una misma persona para la aprobación de órdenes de compra y la tramitación de pagos). El principio se aplica a la división de roles en el desarrollo y las operaciones del *Cloud*, así como al ciclo de vida del software. Un ejemplo en el ámbito del desarrollo de software en *Cloud* sería la segregación de los desarrolladores del personal que opera los sistemas, garantizando además que no existen puertas traseras no autorizadas en el producto final. Los diferentes componentes de las infraestructuras críticas deben ser gestionados por personal diferente. Adicionalmente, la concesión al personal de únicamente aquellos privilegios que necesita para el desarrollo de sus funciones reducirá considerablemente el riesgo, pero no lo eliminará.

La segregación de funciones y la reducción de privilegios/accesos son principios que ayudan al proveedor de *Cloud* a alcanzar el objetivo de proteger y aprovechar los activos de información de la organización. Un programa de gestión de la seguridad *Cloud* requiere la asignación de roles y responsabilidades clave, que pueden recaer en individuos o grupos. Estos roles y responsabilidades deben ser definidos formalmente en el marco de la política de seguridad de la información, debiendo ser revisados y aprobados formalmente por la alta dirección, en línea con sus responsabilidades fiduciarias de GRC (*Governance, Risk and Compliance* – Gobierno, Riesgo y Cumplimiento).

Adicionalmente, el desarrollo de una seguridad de recursos humanos efectiva debe incluir acuerdos con los empleados, acuerdos de confidencialidad, verificaciones de antecedentes (cuando estén legalmente permitidos) y un adecuado proceso de contratación y cese. Otras medidas adicionales que se pueden considerar, en caso de que sean aplicadas en todas las áreas de la organización, incluyen descripciones formales de los puestos, formación adecuada, autorizaciones de seguridad, rotación de puestos y vacaciones obligatorias para el personal más sensible o con roles de alto riesgo.

³³ Según se describen y usan en otros estándares como, por ejemplo, CoBIT 4.

7.3 Evaluando la Seguridad del CSP

Algunos de los riesgos de seguridad asociados con *Cloud computing* son únicos, debido parcialmente a la ampliación de una cadena de custodia de datos centralizada. En este contexto, la continuidad de negocio, la recuperación ante desastres y los entornos de seguridad tradicional de un proveedor de servicios de *Cloud* deben ser evaluados a fondo, y de acuerdo a los estándares de la industria.

La Seguridad Tradicional o Física de las instalaciones del proveedor de servicios de *Cloudes* importante, por lo que necesita ser evaluada a fondo considerando diferentes parámetros. Esta es un área de alta similitud, dado que los requerimientos de seguridad de un CPD con plataformas con *Cloud*, o un CPD tradicional son bastante similares.

Una visión holística y un entendimiento del modelo o filosofía “personas, procesos, tecnología” en un CSP ayudarán inmensamente en la evaluación de la madurez del CSP, e identificarán cuestiones abiertas que deberán ser resueltas, aprobadas y cerradas antes de proceder.

La madurez organizacional y la experiencia contribuyen mucho de cara a la gestión efectiva de los programas de seguridad física, así como de las contingencias que puedan aparecer. Invariablemente, existe un fuerte componente humano envuelto en la administración efectiva de los programas de seguridad física. El nivel de apoyo de la dirección y el calibre del liderazgo en seguridad son factores significativos para la protección de los activos de la compañía, siendo crítico el apoyo de la dirección.

La seguridad física es generalmente la primera línea de defensa contra accesos autorizados y no autorizados a los activos físicos de la organización, así como contra el robo físico de registros, venta de secretos, espionaje industrial y fraude.

7.3.1 Procedimientos

Los proveedores de servicios de *Cloud* deben asegurarse de que la siguiente documentación está disponible para la revisión por parte de sus clientes:

- Verificación de antecedentes (una vez al año) por parte de terceros.
- Acuerdos de confidencialidad (NDA).
- Implementar políticas de compartición de información basadas en limitar a los usuarios los privilegios de acceso y el acceso a la información en base a sus necesidades reales.
- Separación de funciones.
- Administración de los accesos de usuarios.
- Descripciones de los puestos (Roles y Responsabilidades).
- Sistema de control de acceso basado en roles.
- Revisiones de los accesos de los usuarios.

7.3.2 Personal de Seguridad

En caso de que sean necesarias la monitorización e intervención humanas, la plantilla de seguridad física compuesta de guardias, supervisores y oficiales deberá estar 24 x 7 en las instalaciones del CSP.

Entre otras cosas, las instrucciones de las instalaciones y de los puestos deben incluir lo siguiente:

- Verificar las credenciales de empleados, contratados y visitantes, así como el uso de un registro de accesos.
- Revisar y recuperar las tarjetas de identificación de los visitantes.
- Controlar posibles accesos no autorizados que hagan uso, por ejemplo, de ingeniería social, para “colarse” en las instalaciones
- Controlar a los visitantes y sus movimientos en las instalaciones.
- Gestionar las llamadas telefónicas relevantes para la seguridad.
- Monitorizar los sistemas de intrusión, prevención de incendios y asignación de personal para dar respuesta a alarmas.
- Controlar el movimiento de materiales dentro y fuera del edificio, respetando la regulación en materia de movimiento de materiales.
- Respetar las reglas y regulaciones establecidas en el edificio.
- Patrullar el interior de las instalaciones.
- Monitorizar el CCTV.
- Control y gestión de llaves.
- Ejecutar procedimientos de respuesta ante emergencias.
- Escalar las cuestiones de seguridad al responsable de seguridad.
- Recibir y distribuir el correo.
- Acompañar a los visitantes que no hayan sido atendidos a la oficina.

7.3.4 Seguridad Medioambiental

Las instalaciones de los CSP deberían proteger tanto al personal como a los activos mediante la implementación de controles que protejan el entorno de peligros medioambientales. Estos controles pueden incluir, entre otros, los siguientes: controles de temperatura y humedad, detectores de humo y sistemas de supresión de incendios.

7.3.4.1 Controles Medioambientales

- El CPD debe estar equipado con medidas de seguridad medioambiental específicas, de acuerdo a los estándares internos, locales y/o regionales o de acuerdo a la legislación regional, incluyendo un suministro de emergencia/ininterrumpido de energía.
- El equipamiento/dispositivos necesarios para los controles medioambientales debe estar protegido para reducir el riesgo derivado de amenazas y peligros medioambientales, así como el riesgo derivado de accesos no autorizados a la información.

7.3.4.2 Ubicación y Protección del Equipamiento

Los siguientes controles deben ser considerados para aquellos sistemas que contengan información restringida o confidencial:

- El equipamiento está ubicado en una localización física segura que minimice los accesos innecesarios.
- Las condiciones medioambientales, como la humedad, que puedan afectar negativamente a la operativa de los sistemas informáticos, se encuentran monitorizadas.
- El personal de seguridad debería tener en cuenta el impacto potencial que pueda causar un desastre cercano, (i.e. fuego en un edificio aledaño) filtraciones de agua desde el tejado o en plantas inferiores, o una explosión en la calle.
- Empleo de métodos que aseguren la correcta destrucción de los dispositivos descartados (i.e. discos duros).

7.3.4.3 Mantenimiento del Equipamiento

El mantenimiento apropiado del equipamiento se debe realizar a través de controles que garanticen la disponibilidad e integridad continuadas. Dichos controles deben incluir:

- Mantener el equipamiento de acuerdo con los intervalos de servicio y especificaciones recomendados por el proveedor.
- Permitir únicamente al personal de mantenimiento llevar a cabo las reparaciones necesarias sí la gestión de nuevo equipamiento.
- Almacenar un registro de fallos, supuestos o reales, y del mantenimiento preventivo y correctivo.
- Usar controles apropiados durante el envío del equipamiento fuera de las instalaciones para su mantenimiento. Ejemplos de controles apropiados incluyen: el empaquetamiento y sellado de contenedores, el almacenamiento en lugares seguros, e instrucciones de envío y seguimiento claras y completas.
- Mantener apropiadamente políticas y procedimientos para el control de activos, incluyendo la conservación de registros para todo el hardware, firmware y software que engloben trazabilidad, responsabilidad y propiedad.

Una revisión en profundidad de las instalaciones de los CSP permitirá al potencial cliente llevar a cabo un entendimiento y una evaluación acerca de la madurez y experiencia del programa de seguridad. Generalmente, puesto que el foco se sitúa sobre la seguridad IT, la seguridad física recibe atención limitada. No obstante, teniendo en cuenta el amplio abanico de escenarios de amenazas frecuentes hoy en día, la seguridad física adquiere mayor importancia,

especialmente en un entorno en el que la información de los clientes puede cohabitar con la de otros clientes (incluyendo competidores). La Seguridad Física es una de las muchas líneas interconectadas de defensa contra intrusos y saboteadores corporativos que pretenden obtener acceso a las instalaciones del CSP para realizar actividades maliciosas.

7.4 Continuidad de Negocio

Tradicionalmente, los tres principios de la seguridad de la información eran confidencialidad, integridad y disponibilidad; la Continuidad de Negocio está relacionada con la continuidad de dichos tres elementos. La migración a un Proveedor de *Cloud Computing* debe incluir una evaluación del tiempo de disponibilidad al cual el proveedor se ha comprometido por contrato. Sin embargo, este Acuerdo de Nivel de Servicio (ANS) puede no ser suficiente para satisfacer al cliente, por lo que, por ejemplo, se debe tener en consideración el potencial impacto que puede originar un apagón significativo. En base a recientes interrupciones de servicios de alto perfil en servicios externalizados a terceros, los autores sugieren que el mantenimiento de la continuidad del servicio es un aspecto crítico del negocio que permiten mantener la continuidad de las operaciones.

Las siguientes directrices deben ser consideradas a la hora de mantener la continuidad de un servicio dado. Aunque muchas de estas directrices aplicarían probablemente también a servicios internos como si estuvieran externalizados a terceros (i.e. *Cloud*), deben estar formalizadas con el pretexto de que la responsabilidad recaiga en el tercero.

7.5 Recuperación de Desastres

Uno de los aspectos más interesantes del almacenamiento en *Cloud* para IT es la manera en la cual se puede aprovechar para gestionar las copias de seguridad y la recuperación ante desastres (DR – *Disaster Recovery*). Las copias de seguridad en *Cloud* y los servicios de DR tienen como objetivo la reducción de los costes de infraestructura, aplicaciones y del conjunto de procesos de negocio, permitiendo un nivel de protección asequible y fácil de gestionar. Algunos de los retos del almacenamiento en *Cloud*, las copias de seguridad en *Cloud* y el DR en particular incluyen la movilidad, las transferencias de información desde y hacia *Cloud*, la disponibilidad, asegurar una óptima continuidad de negocio, la escalabilidad y una facturación de servicios basada en parámetros medibles. Las soluciones de recuperación ante desastres en *Cloud* se construyen en base a tres fundamentos: una infraestructura de almacenamiento completamente virtualizada, un sistema de archivos escalable y una aplicación de recuperación ante desastres personalizable y fiable que responda a los requerimientos urgentes del negocio.

Los clientes que migren la recuperación ante desastres a *Cloud*, deben verificar la existencia de las siguientes organizaciones o equipos dentro del plan de recuperación ante desastres del proveedor:

- Equipo de Respuesta de Emergencia.
- Equipo de Gestión de Crisis.
- Equipo de Respuesta ante Incidentes.

La composición de los equipos anteriormente citados debe ser revisada en detalle, así como el procedimiento de comunicación de crisis.

7.5.1 Prioridades de la Restauración

Se debe revisar la documentación del proveedor relativa al plan de restauración del servicio; este plan debe incluir el detalle de las diferentes prioridades de la secuencia de restauración. Debe existir una correlación directa con el ANS, de acuerdo a lo comprometido por contrato, relativa a los servicios adquiridos por el cliente y a su criticidad. El Plan de Restauración debe contar y cuantificar el **RPO**³⁴ y el **RTO**³⁵ para cada uno de los servicios.

El detalle de los controles de seguridad de la información que son considerados e implementados durante el proceso de restauración, debe incluir, a modo de ejemplo:

- Autorización del personal envuelto en el proceso de restauración.
- Controles de seguridad física implementados en la localización alternativa.
- Dependencias específicas que sean relevantes en el proceso de restauración (proveedores y terceros).
- Separación mínima a la que se debe situar la localización secundaria en caso de que la primaria no esté disponible.

7.6 Permisos

- Asegurar el diseño adecuado de las instalaciones.
- Disponer de sistemas integrados de seguridad física y lógica que se refuercen mutuamente.
- Establecer acuerdos de nivel de servicio que requieran que las obligaciones de seguridad y obligaciones de los empleados se hereden hacia niveles más bajos del proceso de provisión del servicio.

7.7 Recomendaciones

7.7.1 Recomendaciones para las Políticas

- Los proveedores de *Cloud* deben considerar como directrices de seguridad la adopción de los requerimientos más restrictivos en caso de que algún cliente cuente con sistemas, instalaciones y procedimientos catalogados como nivel alto. Siempre y cuando las medidas de seguridad más restrictivas no impacten negativamente en la satisfacción del cliente, deberían resultar rentables y cuantificables, a través de la reducción del riesgo del personal, ingresos, reputación y valor de los accionistas.
- Alternativamente, los proveedores se pueden orientar a un conjunto de usuarios con menores requerimientos de seguridad u ofrecer un nivel básico para todos los clientes con la posibilidad de implementar medidas adicionales para aquellos que lo valoren. En el segundo caso, se deberá ser consciente de que algunos clientes estarán interesados sólo en aquellos proveedores que provean un nivel de seguridad uniforme. En este acto de ponderación se deben considerar sistemas, instalaciones y procedimientos documentados.

³⁴ **RPO** - *Recovery Point Objective* - Punto Objetivo de Recuperación

³⁵ **RTO** - *Recovery Time Objective* - Tiempo Objetivo de Recuperación

- Los proveedores deberían contar con una diferenciación clara de las responsabilidades de cada puesto, realizar verificaciones de antecedentes, solicitar acuerdos de confidencialidad para empleados, y restringir el conocimiento de los empleados acerca de los clientes a lo mínimo necesario.

7.7.2 Recomendaciones de Transparencia

- Se debe solicitar al CSP transparencia en relación con su enfoque de seguridad. Una visita a las instalaciones del CSP o a su CPD ayudarán a realizar una evaluación presencial, y a obtener un entendimiento claro acerca de las diferentes medidas que han sido implementadas. No obstante, debido a las características de la provisión bajo demanda y el uso compartido de los recursos del *Cloudcomputing*, los procesos tradicionales de evaluación y auditoría pueden no ser idóneos, o pueden requerir modificaciones (i.e. compartir el acceso a una inspección de un tercero).
- De cara a aumentar la efectividad de la evaluación presencial, la visita a las instalaciones del CSP o a su CPD debería ser realizada sin previo aviso (se puede sino informar al CSP acerca de su realización en un rango amplio de fechas, en vez de fechas específicas). Esto posibilitará la realización de una evaluación real sobre el terreno en un día ordinario en vez de dar la oportunidad al CSP de “mantener las apariencias” a lo largo de la visita de un cliente o tercero.
- Si se persigue una evaluación directa, el equipo evaluador debería componerse de al menos dos miembros con experiencia en funciones de IT, Seguridad de la Información, Continuidad de Negocio, Seguridad Física y Dirección (i.e. directores de departamento o propietarios de datos).
- Los clientes deberían solicitar y obtener la documentación relativa al plan de continuidad de negocio y plan de recuperación de desastres antes de la visita, incluyendo las certificaciones relevantes (i.e. ISO, **ITIL**) así como los informes de auditoría y protocolos de test.

7.7.3 Recomendaciones de Recursos Humanos

- Los clientes deberían verificar si el CSP cuenta con personal de seguridad competente para la función de seguridad física. Es altamente recomendable la dedicación exclusiva de un gerente que aporte el liderazgo necesario y que gestione los programas de seguridad física. Las principales certificaciones de la industria como **CISA**³⁶, **CISSP**³⁷, **CISM**³⁸, **ITIL**, o **CPP**³⁹ (de **ASIS**⁴⁰) contribuyen a la hora de verificar la experiencia, conocimientos y habilidades en Seguridad física del personal involucrado.
- Los clientes deberían requerir una revisión profunda de la estructura de reporte al gerente responsable de seguridad. Esto ayudaría a determinar si el puesto ha sido otorgado de acuerdo a su importancia y responsabilidades. El gerente responsable de seguridad debería reportar a un supervisor funcional y a su Comité de GRC, en caso de que exista, no debiendo responder a Infraestructuras o IT. Lo mejor, en términos de

³⁶ **CISA** - *Certified Information Security Auditor*

³⁷ **CISSP** - *Certified Information System Security Professional*

³⁸ **CISM** - *Certified Information Security Manager*

³⁹ **CPP** - *Certified Privacy Professional*

⁴⁰ **ASIS** - *American Society for Industrial Security*

independencia y objetividad del puesto, sería que este puesto reportase al CEO a través de otra cadena de mando, (i.e. a través del CRO o del consejo de dirección).

7.7.4 Recomendaciones de Continuidad de Negocio

- Los clientes deberían revisar los contratos de los compromisos adquiridos por terceras partes para asegurar la continuidad del servicio externalizado. No obstante, el cliente debería sopesar la necesidad de realizar un análisis en mayor profundidad. Típicamente el cliente actúa como propietario de los datos, y en aquellos casos en los que se traten datos de carácter personal, es probable que existan requerimientos regulatorios específicos para asegurar la adecuada implementación de controles. Dichos requerimientos regulatorios aplican incluso en el caso de que un tercero procese los datos.
- El cliente debería revisar el Plan de Continuidad del tercero, así como cualquier certificación. Por ejemplo el CSP puede estar certificado en ISO 22301 o BS 25999, Estándares Internacionales para la Gestión de la Continuidad de Negocio (BCM – *Business Continuity Management*). El cliente puede preferir revisar el alcance de la certificación y la documentación detallada de la evaluación.
- El cliente debería llevar a cabo una evaluación presencial en las instalaciones del CSP para confirmar y verificar la existencia de los controles mencionados que se utilizan para mantener la continuidad del servicio. Dicha evaluación puede ser realizada tras una notificación previa, siempre que se realice única y exclusivamente para verificar los controles del BCP, ya que típicamente estos controles sólo se ejecutarían en caso de que ocurriera un desastre.
- El cliente debería asegurarse de que recibe información de cualquier prueba que se realice del BCP/DR. Mientras que muchas de las recomendaciones que ya han sido mencionadas anteriormente se focalizan en el análisis documental y de procedimientos, la auténtica prueba es la ocurrencia de un desastre. Sin que ello tenga que ocurrir, el cliente debe subrayar la importancia de obtener confirmación formal de la realización de las pruebas del BCP/DR, así como del grado de cumplimiento de los ANS acordados a nivel contractual.

7.7.5 Recomendaciones de Recuperación de Desastres

- Los clientes de *Cloudno* deberían depender de un único proveedor de servicios y deberían contar con un plan de recuperación de desastres que facilite la migración en caso de que falle un proveedor.
- Los proveedores de IaaS (Infrastructure as a Service) deberían contar con acuerdos contractuales con múltiples proveedores de plataformas y con herramientas para restaurar rápidamente los sistemas en caso de pérdida.
- La validación de datos debería ser un protocolo automático o validado por el usuario que permita al cliente verificar sus datos en cualquier momento y asegurar así su integridad.
- Las copias de seguridad incrementales deberían replicar frecuentemente los sistemas mejor protegidos, o bien disponer de copias completas para cada sistema en los intervalos que establezca el usuario. De esta manera el cliente determina la configuración de acuerdo a los puntos objetivos de recuperación.
- El sitio completo, el sistema, el disco y la recuperación de ficheros deberían estar accesibles a través de un portal personalizado que permita flexibilidad al usuario a la hora de elegir el fichero o sistema a recuperar.

- El proveedor de *Cloud* debería implementar ANS ágiles basados en la recuperación de información.
- Los ANS deberían ser negociados por adelantado y el cliente debería pagar por los ANS solicitados para asegurarse que no hay conflicto de intereses. Ningún dato, fichero o disco debería tardar más de 30 minutos en ser recuperado.
- La WAN entre el cliente y las instalaciones físicas debe ser desplegada y optimizada de tal manera que permita movilidad total de los datos con un mínimo ancho de banda, almacenamiento y coste.

7.8 Requerimientos

- ✓ Todas las partes deben asegurar un adecuado diseño estructural para la seguridad lógica.
- ✓ Todos los participantes en el proceso de provisión del servicio deben respetar la interdependencia entre las soluciones de disuasión, detección y autenticación.
- ✓ Los clientes finales deben inspeccionar, justificar y resolver los riesgos propios heredados de otros miembros de la cadena de provisión del servicio *Cloud*. Asimismo, deben diseñar e implementar medidas activas que mitiguen y contengan dichos riesgos propios, a través de una adecuada segregación de funciones, y la concesión a los empleados únicamente de aquellos privilegios que requieran para el desarrollo de sus funciones.

DOMINIO 8 //

ACTIVIDADES DEL CPD

Para que pueda haber una evolución del *Cloud Computing*, el proveedor debe promover el CPD empresarial más allá del simple uso de la virtualización para gestionar los activos del servidor. Para permitir la agilidad en el negocio, la tecnología verde, la transparencia del operador, las ideas cada vez más singulares de la generación de energía y la construcción y gestión del CPD, éste tiene que transformarse para que el uso de *Cloud*, a largo plazo, tenga éxito.

“*Next Generation Data Center*” (“Próxima Generación de CPDs”), un término que ha sido utilizado durante varios años, se ha desarrollado como el conjunto de actividades del CPD que incluye la aplicación de inteligencia de negocio en el CPD, entendimiento de las aplicaciones que se ejecutan en él, así como también la evolución de los requerimientos de alojamiento a gran escala de los *clusters* analíticos. El CPD no es una entidad independiente sino una entidad que tiene que ser tan ágil como las aplicaciones y también debe estar conectada a otros CPDs para poder gestionar la latencia, así como la seguridad.

Introducción. En este capítulo se abordarán los siguientes temas:

- Consideraciones de seguridad física en relación a la CCM
- Mapeo de los casos de uso de CPDs automatizados
- ¿El nuevo CPD? *Cloud Computing* en el hogar
- Difusión de infraestructura de *Cloud* y el CPD

Consideraciones de CCM y cómo impactan con las nuevas ideas en los CPDs de Cloud

8.1 Actividades del CPD

Nuevos conceptos en esta sección:

- **Objetivo de la aplicación de *Cloud*.** El objetivo de la industria o de la aplicación alojada en el CPD. Por ejemplo, el objetivo de una aplicación podría ser el cuidado de la salud o el comercio electrónico.
- **Difusión de los CPDs.** Infraestructuras de *Cloud* que operan conjuntamente pero están separadas físicamente.

Los servicios basados en la automatización y el análisis predictivo para permitir la automatización basada en servicios, han sido representados durante mucho tiempo por **ITSM**⁴¹ utilizando los estándares de **ITIL** para la evolución de los CPDs. Los distintos tipos de aplicaciones alojadas en los CPDs requieren ser automatizadas. Aquellos que gestionan los CPDs se benefician en gran medida al entender lo que se está ejecutando en su interior y cómo el CPD en su conjunto necesita poder responder a un uso variable y dinámico.

La matriz de controles de *Cloud* de la *Cloud Security Alliance* tiene una serie de requisitos físicos basados en diferentes estándares y requisitos regulatorios. El dominio de la seguridad física en esta versión de la guía y la CCM, deberían ser leídos por los profesionales relacionados con los CPDs para obtener un entendimiento de los requisitos internos y

⁴¹ **ITSM** - Information Technology Service Management (Gestión de Servicios de Tecnologías de la Información)

externos de dichos CPDs. Como referencia, la siguiente tabla ilustra los controles que necesita el CPD, basados en el objetivo de las aplicaciones alojadas en el mismo. La tabla no es exhaustiva pero incluye algunos ejemplos de referencias cruzadas entre la CMM y las especificaciones de la aplicación según el tipo o el objetivo/función de la misma.

Tabla 6— Misión de la Aplicación por Control

MISIÓN DE LA APLICACIÓN	CONTROL	ESPECIFICACIÓN
Cuidado de la salud (HIPAA⁴²)	Seguridad de las instalaciones— Política de Seguridad	Las políticas y procedimientos se establecerán para mantener un ambiente de trabajo seguro en oficinas, salas, instalaciones y áreas seguras.
Procesamiento de tarjetas/Pagos (PCI)	Seguridad de las instalaciones – Acceso de los usuarios	El acceso físico a los activos de información y a las funciones de usuarios y personal de soporte será restringido.
Generación de energía (NERC CIP⁴³)	Seguridad de las instalaciones – Puntos de acceso controlados	Deberán reforzarse los perímetros de seguridad física (vallas, muros, barreras, puertas, guardias, vigilancia electrónica, mecanismos de autenticación física, servicios de recepción y patrullas de seguridad) para proteger los datos sensibles y los sistemas de información.

La lista anterior no pretende ser exhaustiva en este capítulo. El lector puede revisar la matriz y seleccionar los controles en base a los estándares a los que la organización quiere adherirse o la regulación que la compañía debe cumplir.

Se auditarán las aplicaciones que se ejecuten en el CPD y que contengan información regulada (que se rige por un estándar de seguridad de la información o de seguridad de las aplicaciones). El resultado de las conclusiones de las auditorías físicas realizadas por el operador del CPD puede ser publicado para los clientes del operador de dicho CPD o incluirse en una infraestructura de consultas sobre aplicaciones, como la proporcionada por la Auditoría de *Cloud*.

En las versiones anteriores de la Guía, se instruyó al lector para llevar a cabo sus propias auditorías. Para muchos operadores de CPD o proveedores de *Cloud* esto no es físicamente posible. En entornos *multi-tenant* el operador o proveedor no podría recibir las visitas de cada cliente para llevar a cabo su auditoría. El cliente debe exigir al operador o proveedor que le proporcione los resultados de una auditoría independiente.

Esta idea deriva en la automatización de los servicios. Mediante la automatización de los informes, los registros y la publicación de los resultados de la auditoría, el operador del CPD puede proporcionar a sus clientes evidencias que, basadas en el objetivo de la aplicación, indiquen que los controles específicos están implementados y son satisfactorios. La auditoría de *Cloud*, el *Cloud Trust Protocol* y CYBEX (X.1500) pueden automatizar la publicación de hallazgos de auditoría a través de un interfaz accesible común.

Una mayor automatización en el CPD dependería de la biblioteca que contiene los activos alojados en el CPD. Según cómo los activos de la librería utilicen los recursos del CPD, la gestión de las operaciones podría predecir qué clientes

⁴² HIPAA - Healthcare Information Portability and Protection Act

⁴³ NERC CIP - North American Electric Reliability Corporation Critical Infrastructure Protection

utilizarán los recursos. Si el CPD utiliza conceptos como **PoDs**⁴⁴ y **VMDC**⁴⁵, entonces el CPD será tan ágil como puede ser la promoción del *Cloud* o la rápida virtualización del negocio.

8.1.1 Modelos nuevos y emergentes

Recientemente (en verano de 2011) hubo bastantes noticias sobre plataformas *Cloud* de particulares. En estos tipos de infraestructuras siguiendo el modelo de **SETI@home**⁴⁶, un *Cloud* está basado en los activos de voluntarios que exponen los recursos informáticos de su casa u oficina para dar soporte a otras aplicaciones. Los CPDs en estos casos son las casas de dichos voluntarios. Estos tipos de *Clouds* trabajarían bien como entornos de alojamiento de aplicaciones basados en comunidades, pero no como entornos regulados donde los estándares son auditados. Por ejemplo, si un *Cloud* está alojado en 100.000 ordenadores de casa, no habrá modo de auditar un CPD que realmente esté dividido en 100.000 piezas y que además estén dispersas por una amplia área geográfica. Este tipo de infraestructura podría alojar un conjunto de aplicaciones comunitarias basadas en intereses (por ejemplo un club de lectura) o en un sitio web residencial.

El *cCloud* cada vez se ve más como un bien o un servicio público. Se realizan esfuerzos en la industria para crear SecaaS o crear infraestructuras de intermediarios (*broker infrastructures*) para la identidad, interoperabilidad y continuidad de negocio, entre otras razones. La aplicación entonces se separa y se coloca en entornos físicos especializados que se centran en las necesidades específicas de una organización o en las aplicaciones que se ejecutan.

La difusión del CPD consiste en colocar la aplicación en varios CPDs especializados que alojan y gestionan las necesidades específicas. Gracias a esta difusión a través de las fronteras físicas, la aplicación sobrecarga menos el *Cloud* pero es más difícil de controlar y gestionar.

8.2 Permisos

- Difusión de la colaboración del CPD. La automatización del CPD abarcando varios CPDs no relacionados físicamente entre sí, requiere de un software para organizar las necesidades del CPD para el registro y la generación de informes durante las auditorías.
- *Clouds* de particulares donde el CPD es personal. La auditoría de los estándares y el cumplimiento legal son casi imposibles en estas *clouds*. Los entornos regulados y los basados en estándares tendrán dificultades con las *clouds* de particulares si nos apoyamos en los controles necesarios. Pueden darse situaciones en las que alguna parte de la aplicación podría estar difundida en una infraestructura *Cloud* de particulares.

8.3 Recomendaciones

- Las organizaciones que construyen CPDs en *Cloud*, deberían incorporar procesos de gestión, prácticas y software para entender y reaccionar a la tecnología que se ejecuta en el CPD.

⁴⁴ **PoD** - Point of Delivery. Un conjunto de potencia, cálculo, almacenamiento de acceso y componentes de red contenidos en una sola unidad.

⁴⁵ **VMDC** - Virtual Multi-tenant Data Center. Un concepto basado en la utilización de componentes modulares y fácilmente enracables, para expandir rápidamente un CPD tales como PoDs

⁴⁶ **SETI@home** - <http://setiathome.berkeley.edu/>

- Las organizaciones que compran servicios de *Cloud* deberían asegurarse de que el proveedor ha adoptado procesos de gestión del servicio y prácticas para utilizar sus CPDs y han adoptado técnicas de enrackado que aseguran agilidad y alta disponibilidad en las fuentes del propio CPD.
- Entender la función de las aplicaciones que se ejecutan en el CPD. Teniendo en cuenta los controles de la CCM , el CPD construido o adquirido debe cumplir con los requisitos de seguridad física y de seguridad de los activos.
- Las localizaciones del CPD son importantes. Si los componentes de la tecnología y de la aplicación se distribuyen en los CPDs, entonces habrá periodos de latencia entre los mismos.
- Las organizaciones que compran servicios en *Cloud* deberán entender claramente y documentar quiénes son los responsables para cumplir con los requisitos de cumplimiento legal y los roles que ellos y su proveedor de *cloud* deben tener al evaluar el cumplimiento legal.

8.4 Requisitos

Cloud Security Alliance cuenta con muchas fuentes de información para ayudar en la construcción y la remodelación de los CPDs para el *Cloud*. La matriz de controles destaca los requisitos a través de un amplio conjunto de estándares de seguridad y regulaciones. La auditoría del *Cloud* y de otros proyectos dentro de CSA también puede ayudar con la construcción de los CPDs y la tecnología que albergarán.

- ✓ Entender totalmente los requisitos de la CCM basados en lo que se va a ejecutar en el CPD. Usar un denominador común que satisfaga los objetivos de la mayoría de las aplicaciones.
- ✓ Utilizar técnicas de gestión de servicios de TI para asegurar la disponibilidad, seguridad y entrega y gestión de activos.
- ✓ Si el CPD pertenece a un proveedor, la auditoría reglamentaria y de seguridad se realizará mediante una plantilla y se publicarán los resultados para que disponga de ellos el cliente.

DOMINIO 9 //

RESPUESTA ANTE INCIDENTES

La respuesta ante incidentes (IR) es una de las piedras angulares de la gestión de la seguridad de la información. Hasta la planificación, implementación y ejecución de los controles de seguridad preventiva más diligentes no pueden eliminar la posibilidad de un ataque a los activos de la información. Por lo tanto, una de las cuestiones centrales para las organizaciones que se mueven a *Cloud* debe ser: ¿qué se debe hacer para permitir el manejo eficiente y eficaz de los incidentes de seguridad que involucran a los recursos en *Cloud*?

El *Cloud computing* no necesita un nuevo marco conceptual para la respuesta ante incidentes; sino que requiere que la organización adapte adecuadamente sus programas, procesos y herramientas de respuesta ante incidentes existentes al entorno operativo específico que va a abrazar. Esto se alinearán con la guía encontrada a lo largo de este documento; un análisis de deficiencias en los controles que abarcan la respuesta ante incidencias de las organizaciones debe llevarse a cabo de la misma manera.

Este dominio busca identificar las lagunas pertinentes en la respuesta ante incidentes que son creadas por las características únicas del *Cloud computing*. Los profesionales de la seguridad pueden usar esto como referencia cuando desarrollen planes de respuesta y conduzcan otras actividades durante la fase de preparación del ciclo de vida de la respuesta ante incidentes. Para comprender el desafío que supone el *Cloud computing* para la gestión de incidentes, debemos examinar qué desafíos suponen para la gestión de incidentes las características especiales del *Cloud computing*, los diferentes tipos de despliegues y modelos de servicio.

Este dominio está organizado en acuerdo con el comúnmente aceptado ciclo de vida para respuesta ante incidentes como está descrito en el *National Institute of Standards and Technology Computer Security Incident Handling Guide (NIST 800-61) [1]*. Después de establecer las características del *Cloud computing* que impactan la respuesta ante incidentes de manera más directa, cada sección posterior aborda una fase del ciclo de vida y explora las consideraciones potenciales de los **Equipos de respuesta**.

Introducción. En este capítulo se abordarán los siguientes temas:

- Impacto del cloud computing en la respuesta ante incidentes
- Ciclo de vida de la respuesta ante incidentes
- Responsabilidad Forense

9.1 Características del *Cloud Computing* que impactan en la respuesta ante incidentes

Aunque *Cloud computing* trae cambios a muchos niveles, algunas características [2] del *Cloud computing* soportan más desafíos directos a las actividades de IR que otras [3].

En primer lugar, la naturaleza de la demanda de auto-servicio en los entornos de *Cloud computing* significa que un cliente de *Cloud* puede encontrar difícil o incluso imposible recibir la cooperación necesaria por parte de su proveedor de servicios de *Cloud* (CSP) al manejar un incidente de seguridad. Dependiendo de los modelos de servicio y de despliegue utilizados, la interacción con la función de RI en el CSP pueden variar. De hecho, el grado en que se hagan

considerado en la oferta de servicios aspectos como las capacidades de detección de incidentes de seguridad, el análisis, la contención y la recuperación son cuestiones clave.

En segundo lugar, la agrupación de recursos practicados por servicios en *Cloud*, además de la rápida elasticidad ofrecida por las infraestructuras de *Cloud*, puede complicar dramáticamente el proceso de RI, especialmente las actividades forenses llevadas a cabo como parte del análisis del incidente. El análisis forense ha de llevarse a cabo en un ambiente altamente dinámico, que desafía las necesidades básicas forenses [4], como el establecimiento del alcance de un incidente, la recogida y atribución de datos, preservando la integridad semántica de los datos, y el mantenimiento de la estabilidad de las pruebas en general. Estos problemas se agravan cuando los clientes de *Cloud* intentan llevar a cabo las actividades forenses, ya que operan en un entorno no-transparente (lo que pone de relieve la necesidad de apoyo por parte del proveedor de *Cloud* como se mencionó anteriormente).

En tercer lugar, la agrupación de recursos practicada por los servicios de *Cloud* deriva en dificultades de privacidad a los co-inquilinos de cara a la recopilación de datos y el análisis de las mediciones y las herramientas asociados a un incidente (por ejemplo, colecta de datos, imágenes de las máquinas, los datos de la red, la memoria y el almacenamiento, etc.) sin comprometer la privacidad de los co-inquilinos. Este es un reto técnico que debe ser abordado principalmente por el proveedor. Corresponde a los clientes de *Cloud* el asegurarse de que su proveedor de servicios de *Cloud* tenga las medidas adecuadas de recogida y separación de datos y que pueda proporcionar el manejo de incidentes de soporte requeridos.

En cuarto lugar, a pesar de no ser descrito como una característica esencial *Cloud*, *Cloud computing* puede conducir a que los datos crucen las fronteras geográficas o jurisdiccionales sin el conocimiento explícito de este hecho por parte del cliente. Las consecuencias jurídicas y regulatorias que se deriven pueden afectar negativamente el proceso de gestión de incidentes, colocando límites a lo que puede o no puede hacer y / o prescribir lo que debe o no se debe hacer durante un incidente en todas las fases del ciclo de vida [5]. Es aconsejable que la organización cuente con representantes de su departamento legal en el equipo de respuesta ante incidentes para proporcionar orientación sobre estos temas.

Cloud computing también presenta oportunidades para los respondedores de incidentes. Los sistemas de monitorización continua de *Cloud* pueden reducir el tiempo que se tarda en realizar un ejercicio de manejo de incidentes o permitir una mejor respuesta a un incidente. Las tecnologías de virtualización, y la elasticidad inherente en las plataformas *Cloud*, pueden permitir una contención y una recuperación más eficiente y eficaz, a menudo con menos interrupciones de servicio de las que se pueden experimentar con tecnologías más tradicionales para centros de datos. Además, la investigación de incidentes puede ser más fácil en algunos aspectos, como las máquinas virtuales se pueden mover fácilmente en entornos de laboratorio donde se pueden realizar análisis de tiempo de ejecución e imágenes forenses y examinarlas.

9.2 El modelo de seguridad de la arquitectura *Cloud* como referencia

En gran medida, los modelos de despliegue y servicio dictan la división del trabajo cuando se trata de RI en el ecosistema de *Cloud*. Utilizando el marco arquitectónico y revisión de los controles de seguridad abogados en el dominio 1 (ver referencia *Cloud* Modelo Figura 2A) puede ser útil identificando qué componentes técnicos y procesos son propiedad de cada una de las organizaciones y en qué nivel de la "pila".

Los modelos de servicio de *Cloud* (IaaS, PaaS, SaaS) difieren notablemente en la cantidad de visibilidad y control que un cliente tiene sobre los sistemas informáticos subyacentes y otras infraestructuras que ofrece el entorno informático.

Esto tiene implicaciones para todas las fases de la respuesta ante incidentes como las tiene para todos los demás dominios de esta guía.

Por ejemplo, en una solución SaaS, es probable que las actividades de respuesta residan casi en su totalidad en el CSP, mientras que en IaaS, un mayor grado de responsabilidad y la capacidad de detección y respuesta a incidentes de seguridad pueden residir en el cliente. Sin embargo, incluso en IaaS hay dependencias significativas en el CSP. Los datos de equipos físicos, dispositivos de red, servicios compartidos, dispositivos de seguridad como cortafuegos y cualquier sistema de gestión del backplane deben ser entregados por el CSP. Algunos proveedores ya están aprovisionando la capacidad para ofrecer esta telemetría a sus clientes y ciertos proveedores de servicios de seguridad gestionada están anunciando soluciones basadas en *Cloud* para recibir y procesar estos datos.

Dadas la complejidades, el modelo de control de seguridad descrito en el dominio 1 (Figura 2B), y las actividades que lleva a cabo una organización para asignar controles de seguridad en su despliegue *Cloud* particular debe informar de la planificación de IR y viceversa. Tradicionalmente, los controles de IR se han preocupado más estrechamente de los requisitos de una organización a alto nivel, sin embargo, los profesionales de seguridad deben tener una visión más holística para ser realmente eficaces. Los responsables de IR deben estar plenamente integrados en la selección, adquisición y despliegue de cualquier control de seguridad técnico que directamente pueda, e incluso indirectamente, afectar a la respuesta. Como mínimo, este proceso puede ayudar en la asignación de roles / responsabilidades durante cada fase del ciclo de vida de IR.

Los casos de uso de *Cloud* (público, privado, híbrido, comunitario) también son consideraciones a tener en cuenta cuando se revisen de las capacidades de IR en la implementación de *Cloud*; la facilidad de acceder a los datos de IR varía para cada modelo de implementación. Debería ser evidente que el mismo continuum de control / responsabilidad existe aquí también. En este dominio, el principal aspecto a valorar son los casos más públicos de IR. Los autores suponen que cuanto más privado es *Cloud*, más tendrá que desarrollar el usuario los controles de seguridad apropiados o que esos los controles los proporcione un proveedor para satisfacción del usuario.

9.3 Examinando el ciclo de vida de la respuesta ante incidentes

NIST 800-61 [1] describe las siguientes etapas principales del ciclo de vida para IR: preparación; detección y análisis; contención, erradicación y recuperación. Esta sección examina los desafíos específicos de *Cloud* para esas etapas y ofrece recomendaciones de cómo alcanzar estos objetivos.

9.3.1 Preparación

Cuando los activos de información son desplegados en *Cloud*, la preparación puede que sea la fase más importante en el ciclo de vida de la respuesta ante incidentes. Identificar los desafíos (y las oportunidades) para IR debería ser un proyecto formal que debe ser llevado a cabo por profesionales de la seguridad informática dentro de la organización de *Cloud* del cliente antes de migrar hacia *Cloud*. Si el nivel de especialización en IR dentro de la organización del cliente es considerado insuficiente, se debería consultar expertos externos. Este ejercicio debería ser llevado a cabo durante cada actualización del plan de respuesta ante incidentes.

En cada fase del ciclo de vida examinada a continuación las cuestiones planteadas y las sugerencias aportadas pueden servir para informar en el proceso de planificación del cliente. La integración de los conceptos discutidos en un plan

documentado formalmente debería servir para impulsar las actividades adecuadas, para remediar las deficiencias y aprovechar las oportunidades.

La preparación comienza con una comprensión y reconocimiento de responsabilidades claro y completo de donde residen los datos del cliente que se encuentran en movimiento y en reposo. Dado que los activos de información de los clientes pueden atravesar los límites organizacionales, y probablemente, los geográficos, se requiere un modelado de amenazas tanto en el plano físico como en el lógico. Los diagramas de flujo de datos que se asignan a los activos físicos, un mapa organizativo de la red y los límites jurisdiccionales pueden servir para poner de relieve las dependencias que pudieran surgir durante una respuesta.

Dado que varias organizaciones están involucradas, los Acuerdos de Nivel de Servicio (**ANS**) y los contratos entre las partes se convierten en el principal medio de comunicar y hacer cumplir las expectativas de las responsabilidades en cada fase del ciclo de vida de IR. Es recomendable compartir los planes de IR con las otras partes y definir y clarificar con precisión la terminología común o poco clara. En la medida de lo posible, las ambigüedades deberían ser aclaradas antes de un incidente.

No es razonable esperar que un CSP cree distintos programas de IR para cada cliente. Sin embargo, la existencia de algunos (o todos) de los puntos siguientes en un contrato o ANS debería dar a la organización del cliente cierta confianza de que su proveedor dispone de cierta planificación previa a la respuesta ante incidentes:

- Puntos de Contacto, canales de comunicación y la disponibilidad de los equipos de IR para cada parte
- Definiciones de incidentes y criterios de notificación, tanto desde el proveedor al cliente como a otras partes externas
- Soporte del CSP al cliente para la detección de incidentes (por ejemplo, datos disponibles de eventos, notificación sobre eventos sospechosos, etc.)
- Definición de roles / responsabilidades durante un incidente de seguridad especificando explícitamente el apoyo prestado a la gestión de incidentes de clientes prestado por el CSP. Ppor ejemplo, apoyo forense a través de la recopilación de datos de incidentes / artefactos, participación / apoyo en el análisis de incidentes, etc..
- Especificación de las pruebas regulares de IR llevadas a cabo por las partes en el contrato y si los resultados se compartirán
- Alcance de las actividades post-mortem. Ppor ejemplo, análisis de causa, informe de IR, integración de las lecciones aprendidas en la gestión de la seguridad, etc.
- Identificación clara de las responsabilidades en torno a la IR entre el proveedor y el usuario como parte del ANS

Una vez que las funciones y responsabilidades se han determinado, el cliente podrá capacitar, equipar y proveer correctamente de recursos a sus equipos de respuesta ante incidentes para manejar las tareas de las que serán directamente responsables. Por ejemplo, si una aplicación controlada por un cliente reside en un modelo PaaS y el CSP se ha comprometido a proporcionar (o permitir la recuperación de) logging específico de la plataforma, es una necesidad obvia contar con las tecnologías / herramientas y el personal disponible para recibir, procesar y analizar los tipos de logs. Para IaaS y PaaS, la aptitud con la virtualización y los medios para llevar a cabo la investigación forense y otras investigaciones en maquinas virtuales será parte integral de cualquier esfuerzo de respuesta. Una decisión acerca de si la experiencia que se requiere es orgánica a la organización del cliente o si se subcontrata a una tercera parte es

algo que se determinará durante la fase de preparación. Tenga en cuenta que la externalización le pide otra serie de contratos / **NDA**s⁴⁷ para gestionar.

Entre todas las partes involucradas, los canales de comunicación deben estar preparados. Las partes deberían considerar los medios por los cuales se transmite información confidencial para asegurarse de que los canales fuera de banda están disponibles y que se usan los esquemas de cifrado para garantizar la integridad y autenticidad de la información. La comunicación durante el IR se puede facilitar mediante la utilización de los estándares existentes para el propósito de compartir los indicadores de compromiso o de participar activamente otra parte en una investigación. Por ejemplo, el formato de intercambio de descripción de objeto de incidentes (**IODEF**)⁴⁸ [6], así como el estándar de la defensa entre redes en tiempo real asociada (**RID**)⁴⁹ [7,8] se desarrollaron en el Internet Engineering Task Force (**IETF**)⁵⁰ y también son incorporados en el proyecto de intercambio de ciberseguridad (**CYBEX**)⁵¹ de la unión Internacional de Telecomunicaciones (**ITU**)⁵². IODEF proporciona un esquema XML estándar para describir un incidente, RID describe un método estándar para comunicar la información sobre incidentes entre las entidades que incluye, al menos, un CSP y sus clientes.

La parte más importante de la preparación para un incidente es poner a prueba el plan. Las pruebas deberían ser a fondo e implicar a todas las partes que puedan estar involucradas en un incidente real. Es poco probable que un CSP tenga recursos para participar en las pruebas con cada uno de sus clientes; por tanto, el cliente debería considerar técnicas de simulación (juegos de rol) como un medio para identificar qué tareas o solicitudes de información son las que tenga que dirigir al CSP. Esta información debe ser usada para las futuras discusiones con el proveedor, durante la fase de preparación. Otra posibilidad es que el cliente quiera participar voluntariamente en cualquier prueba que el CSP pueda haber previsto.

9.3.2 Detección y análisis

La detección oportuna de los incidentes de seguridad y el éxito en el análisis posterior de los hechos (lo que ha sucedido, cómo sucedió, qué recursos se ven afectados, etc) dependen de la disponibilidad de los datos pertinentes y la capacidad de interpretar correctamente los datos. Como se ha indicado anteriormente, *Cloud* ofrece desafíos en ambos casos. En primer lugar, la disponibilidad de datos en gran medida depende de lo que el CSP proporciona al cliente y puede estar limitado por el carácter altamente dinámico de *Cloud computing*. En segundo lugar, el análisis se complica por el hecho de que el análisis, por lo menos en parte, se ve afectado por la falta de transparencia de la infraestructura propia/proveedor, de la cual el cliente, por lo general, tiene poco conocimiento y, de nuevo, por la naturaleza dinámica de *Cloud computing*, a través del cual la interpretación de los datos se vuelve difícil, a veces incluso imposible.

Dejando de lado por un momento las dificultades técnicas de los análisis de los incidentes, la cuestión de cómo una investigación digital en *Cloud* debería llevarse a cabo con el fin de maximizar el valor probatorio (es decir, la credibilidad) de la prueba permanece en gran medida sin respuesta en estos momentos. Por lo tanto, hasta que los casos legales que involucran incidentes en *Cloud* sean más comunes y existan directrices sobre mejores prácticas aceptadas de manera

⁴⁷ **NDA** - Non-Disclosure Agreement (Acuerdo de no divulgación, Acuerdo de Confidencialidad)

⁴⁸ **IODEF** - Incident Object Description Exchange Format

⁴⁹ **RID** - Real-time Inter-network Defense

⁵⁰ **IETF** - Internet Engineering Task Force

⁵¹ **CYBEX** - Cybersecurity Exchange

⁵² **ITU** - International Telecommunication Union's

genera, los resultados de análisis de incidentes de seguridad en *Cloud* corren el riesgo de no poder ser defendidos en los tribunales.

Hasta que las normas, métodos y herramientas para la detección y análisis de los incidentes de seguridad hayan alcanzado a los avances técnicos introducidos por *Cloud*, la detección de incidentes y análisis seguirá siendo especialmente difícil para estos entornos. Los clientes *Cloud* deben hacer frente a este desafío, asegurándose de que tengan acceso a (1) las fuentes de datos e informaciones que sean relevantes para la detección de incidentes / análisis, así como (2) del apoyo adecuado para el análisis forense de incidentes en el entorno *Cloud* que están utilizando.

9.3.3 Fuentes de datos

Como en cualquier servicio IT de integración alojado, el equipo de IR tendrá que determinar el logging adecuado requerido para detectar adecuadamente los eventos anómalos e identificar las actividades maliciosas que afecten a sus activos. Es imperativo para la organización del cliente para llevar a cabo una evaluación de qué logs (y otros datos) están disponibles, cómo se recogen y procesan y, finalmente, cómo y cuándo pueden ser entregados por el CSP.

La principal fuente de datos para la detección y posterior análisis de los incidentes en el lado del cliente es la información de logging. Las siguientes cuestiones relativas a la información de logging deben ser tomadas en consideración:

- **¿Qué información se debe registrar?** Un ejemplo de los tipos de log que pueden ser relevantes son los logs de auditoría (red, sistemas, aplicaciones, roles y accesos de administración de *Cloud*, copia de seguridad y restauración, el acceso de mantenimiento, y la actividad de gestión de cambios), logs de errores (por ejemplo, los mensajes del kernel en los hipervisores, aplicaciones de los sistemas operativos, etc.), los logs de seguridad específicos (registros de los IDS, los registros del firewall, etc.), los logs de rendimiento, etc. Cuando la información de registro existente no es suficiente, fuentes adicionales de log tienen que ser negociadas / agregadas.
- **¿Es la información registrada consistente y completa?** Un buen ejemplo de una fuente de información de logging incoherente es la imposibilidad para sincronizar los relojes de los las fuentes de log. Del mismo modo, si la información está incompleta respecto a la zona horaria en la que los logs se registran hace imposible interpretar correctamente los datos obtenidos durante el análisis.
- **¿Está reflejada adecuadamente la naturaleza dinámica de *Cloud* en la información registrada?** El comportamiento dinámico de los entornos de *Cloud* es también un motivo frecuente de logs inconsistentes y / o incompletos. Por ejemplo, como nuevos recursos de *Cloud* (VM, etc.) son puestos en línea con la demanda de servicio, la información de log producida por el nuevo recurso tendrá que ser añadida al flujo de datos de log existente. Otro problema probable es la imposibilidad de hacer los cambios dinámicos en la información explícita del log del entorno. Por ejemplo, consideremos el caso en el que se registran las solicitudes de un Web Service a un componente determinado de PaaS pero pueden ser atendidas de forma dinámica por una de varias instancias de este servicio. La información incompleta acerca de la cuestión, qué instancia ha atendido qué petición, puede hacer que un análisis preciso sea difícil o imposible, por ejemplo, si el origen del problema de un incidente es un sola instancia comprometida.
- **¿Se alcanzan los requisitos legales?** Los problemas de privacidad respecto a los entornos compartidos, la regulación respecto a los datos registrados en general y la información de identificación personal en particular, etc. pueden poner limitaciones a la hora de recoger, almacenar y usar los datos registrados recopilados. Estas

cuestiones reglamentarias deben entenderse y abordarse para cada jurisdicción en la que se procesan o almacenan los datos de la empresa.

- **¿Qué patrones de retención de logs son requeridos?** Los requisitos legales y de cumplimiento de normativas indicarán los patrones específicos para la retención de logs. Los clientes de *Cloud* deberían comprender y definir las pautas de la extensión en la retención de logs con el fin de cubrir sus necesidades en el tiempo para estar seguros de que cumple con sus requisitos de análisis de incidentes / forenses.
- **¿Están los logs a prueba de manipulaciones?** Asegurarse de que la parte donde se almacenan los registros sea resistente a las manipulaciones es crítico para un análisis legal y forense preciso. Considere como aspectos críticos de este requisito el uso de dispositivos grabables, la separación de los servidores utilizados para el almacenamiento de logs de los servidores de aplicaciones y control de acceso a los servidores que almacenan los logs.
- **¿En qué formato se comunicará la información de logging?** La normalización de datos de logging es un reto considerable. El uso de formatos abiertos (como el emergente CEE [9]) puede facilitar el procesamiento en el lado del cliente.

Un CSP sólo puede detectar algunos incidentes debido a que este tipo de incidentes ocurren dentro de la infraestructura de su propiedad. Es importante señalar que el ANS debe ser tal que el CSP informe a los clientes de manera oportuna y fiable para permitir que se respete el acuerdo de IR. Para otros incidentes (quizás incluso detectables por el cliente) el CSP puede estar en una mejor posición para la detección. Los clientes de *Cloud* deberían elegir a proveedores que asistan de la mejor manera en la detección de incidentes mediante la correlación y filtrado de los datos de logging disponibles.

La cantidad de datos producidos por el despliegue en *Cloud* puede ser considerable. Puede que sea necesario investigar las opciones del CSP con respecto al filtrado de los registros en el servicio *Cloud* antes de que se envíen los datos a los clientes para así reducir los impactos en la red y en el procesamiento de datos interno del cliente. Otras consideraciones incluyen el nivel de análisis o de correlación realizados por el CSP y el cliente *Cloud* para identificar posibles incidentes previos al análisis forense. Si el análisis se realiza en el CSP, el escalado y puntos de traspaso para la investigación del incidente deben ser determinados.

9.3.4 Investigación forense y otros soportes de investigación para análisis de incidentes

Aunque todavía están en una fase inmadura, los esfuerzos ya están en marcha dentro de la comunidad forense para desarrollar las herramientas y protocolos para recoger y examinar artefactos forenses derivados especialmente de los entornos virtualizados; también, el soporte forense necesario para entornos de PaaS y SaaS está siendo objeto de investigación continua.

Es importante que el cliente entienda los requerimientos forenses para la realización de análisis de incidentes, que investigue en qué medida el CSP cumple con estos requisitos, elija un CSP en consecuencia y que este rellene las lagunas restantes. La cantidad de posibles pruebas a disposición de un cliente *Cloud* difiere fuertemente en función del servicio *Cloud* y el modelo de despliegue que tenga.

Para los servicios IaaS, los clientes pueden realizar investigaciones forenses de sus propias instancias virtuales, pero no podrá investigar los componentes de red controlados por el CSP. Por otra parte, las actividades forenses estándar tales como la investigación del tráfico de la red en general, el acceso a los snapshots de la memoria, o la creación de una imagen de disco duro requieren el soporte en la investigación proporcionado por el CSP. Las técnicas forenses avanzadas

habilitadas por la virtualización como la generación de snapshots de los estados de la máquina virtual o la introspección VM en los sistemas vivos requieren el apoyo forense del CSP también.

Con PaaS y SaaS, en los incidentes de seguridad que tengan su causa en la infraestructura subyacente, el cliente *Cloud* es casi totalmente dependiente del soporte para el análisis del CSP y, como se mencionó anteriormente, los roles y responsabilidades en el IR debe ser acordados en el ANS. Con PaaS, la organización cliente será responsable de cualquier código que se implemente en capa de aplicación de *Cloud*. Es necesario un nivel suficiente de registros de aplicaciones para el análisis de incidentes en escenarios donde la causa principal radica en la aplicación (por ejemplo, un error en el código de la aplicación). En este caso, el apoyo del CSP podría ser la forma de facilitar la generación de logs de aplicaciones, el almacenamiento seguro y el acceso seguro a través de una API sólo en modo lectura [10]. Los proveedores de SaaS que generan extensos logs de aplicaciones específicas del cliente y proporcionan un almacenamiento seguro, así como las instalaciones para el análisis facilitarán la carga de IR del cliente. Esto puede reducir los incidentes de nivel de aplicación considerablemente.

Los proveedores que utilizan sus sistemas de gestión para medir el alcance de un incidente e identificar las partes que ha sido objeto de ataques o están siendo objeto de ataque y proporcionan esos datos a sus clientes *Cloud*, mejorarán en gran medida la respuesta en todos los modelos de servicio.

Para prepararse para el análisis de incidentes en un entorno *Cloud* dado, el equipo de IR del cliente debería familiarizarse con las herramientas de información que el proveedor ofrece para ayudar a las operaciones y procesos de IR de su cliente. Los artículos de bases de conocimiento, las preguntas frecuentes, matrices de diagnóstico para incidentes, etc. pueden ayudar a llenar la falta de experiencia que el cliente *Cloud* tendrá con respecto a la infraestructura y sus normas de funcionamiento. Esta información puede, por ejemplo, ayudar al equipo de IR a discriminar las cuestiones operativas de los eventos e incidentes de seguridad reales.

9.3.5 Contención, Erradicación y recuperación

Al igual que con las otras fases de la respuesta ante incidentes, es necesaria una estrecha coordinación con todas las partes interesadas para asegurarse de que las estrategias desarrolladas para contener, erradicar y recuperarse de un incidente son eficaces, eficientes y tienen en cuenta a todas las implicaciones legales y de privacidad. Las estrategias también deben ser coherentes con los objetivos de negocio y deben tratar de minimizar la interrupción de servicio. Esto es mucho más difícil cuando varias organizaciones están involucradas en la respuesta, como es el caso con el *Cloud computing*.

Las opciones para esta fase diferirán dependiendo de la implementación y del modelo de servicio así como del nivel de la pila que fue objeto del ataque. Se pueden emplear múltiples estrategias, posiblemente por diferentes entidades equipadas con diferentes soluciones tecnológicas. Si es posible, deberían llevarse a cabo ejercicios de imaginación en la fase de preparación para prever estas situaciones y debería ser identificado un proceso de resolución de conflictos. Los clientes también deben considerar cómo su proveedor se encargará de los incidentes que afectan al propio proveedor o que afecten a otros clientes sobre una plataforma compartida, además de los incidentes que están directamente dirigidos a su propia organización.

Los usuarios de IaaS son los principales responsables de la contención, erradicación y recuperación de incidentes. eLos casos de uso de *Cloud* pueden tener algunos beneficios aquí. Por ejemplo, aislar las imágenes impactadas sin destruir las pruebas se puede lograr haciendo una pausa en estas imágenes. Como se explica en la introducción, la relativa facilidad

con la que los nodos se pueden apagar y las nuevas instancias ser creadas, puede ayudar a minimizar la interrupción del servicio cuando un parche correctivo debe ser implementado en cualquier código. Si hay problemas con un determinado *Cloud* IaaS, el cliente puede tener la opción de trasladar el servicio a otro, especialmente si se ha implementado una de las soluciones de gestión de meta-cloud.

La situación es más complicada para las implementaciones de SaaS y PaaS. Los usuarios pueden tener poca capacidad técnica para contener un incidente en un PaaS o SaaS que no sea el cierre de acceso de los usuarios y la inspección / limpieza de sus datos cuando estén alojados en el servicio antes de una posterior reapertura. Pero especialmente para SaaS, incluso estas actividades básicas pueden ser difíciles o imposibles sin el apoyo adecuado del CSP, como los mecanismos de control de acceso de grano fino y el acceso directo a los datos del cliente (en vez de a través de la interfaz web).

En todos los modelos de servicios, los proveedores pueden ayudar con ciertas categorías de ataque, como un ataque de Denegación de Servicio (**DoS**)⁵³. Por ejemplo, las pequeñas empresas pueden beneficiarse de las economías de escala, que permiten que las tecnologías de mitigación más costosas, como la protección contra DoS, puedan extenderse a sus páginas web. Como para las etapas anteriores, el grado en que las instalaciones del proveedor serán puestas a disposición del cliente para ayudar a responder a un ataque debería ser identificado en la fase de preparación. Además, las condiciones en las que el proveedor está obligado a proporcionar ayuda para responder a un ataque deberían ser definidas contractualmente.

El ANS y el plan de IR deberían ser lo suficientemente flexibles como para dar cabida a una actividad con las "lecciones aprendidas" después de la recuperación. Un informe de incidentes detallado basado en las actividades de IR será escrito y compartido con las partes impactadas, es decir, entre el cliente *Cloud*, el CSP y otras organizaciones afectadas / involucradas. El Informe de Incidentes debería incluir la línea de tiempo del incidente, el análisis de la causa raíz o vulnerabilidad, las medidas adoptadas para mitigar los problemas y restaurar el servicio y las recomendaciones a largo plazo para una acción correctiva.

Las acciones correctivas suelen ser una mezcla entre las específicas del cliente y las soportadas por el proveedor, y el equipo de respuesta ante incidentes del proveedor debe proporcionar una sección con su perspectiva del incidente y la propuesta de resolución. Después de una revisión inicial del informe del incidente por parte del cliente y del CSP, deberían celebrarse reuniones conjuntas para elaborar y aprobar un plan de remediación.

9.4 Recomendaciones

- Los clientes *Cloud* deben entender cómo el CSP define los eventos de interés frente a los incidentes de seguridad y de qué eventos / incidentes informa el CSP al cliente y de qué manera. La información de los eventos suministrada utilizando un estándar abierto puede facilitar la tramitación de estos informes por parte del cliente.
- Los clientes *Cloud* deben configurar canales de comunicación adecuados con el CSP que se puedan utilizar en caso de un incidente. Los actuales estándares abiertos pueden facilitar la comunicación de incidentes.
- Los clientes *Cloud* debe entender el soporte que proporciona el CSP en el análisis de incidentes, en particular la naturaleza (contenido y formato) de los datos que el CSP proporcionará con fines de análisis y el nivel de

⁵³ DoS - Denial of Service (Denegación de Servicio)

interacción con el equipo de respuesta ante incidentes del CSP. En particular, se debe evaluar si los datos disponibles para el análisis de incidentes satisfacen los requisitos legales relacionados con las investigaciones forenses que puedan ser relevantes para el cliente del *cloud*.

- Especialmente en el caso de IaaS, los clientes *Cloud* deberían aprovechar que la virtualización usada por los CSP ofrece oportunidades para el análisis forense y recuperación de incidentes tales como el acceso / vuelta atrás a los snapshots de los entornos virtuales, introspección de máquinas virtuales, etc.
- Los clientes de *Cloud* deberían aprovechar la virtualización asistida por hardware y los hipervisores bastionados, con capacidades de análisis forense de los CSP.
- Para cada servicio en *Cloud*, los clientes deberían identificar las clases de incidentes más relevantes y elaborar estrategias para la contención, erradicación y recuperación de incidentes, al igual que deben asegurarse que cada proveedor de *Cloud* puede proporcionar la asistencia necesaria para ejecutar dichas estrategias.
- Los clientes *Cloud* deberían obtener y revisar el historial de un CSP en temas de respuesta ante incidentes. Un CSP puede proporcionar recomendaciones de la industria a los clientes existentes sobre su IRP (plan de respuesta ante incidentes).

9.5 Requerimientos

- ✓ Para cada proveedor de servicio en *Cloud*, el enfoque para la detección y el manejo de los incidentes relacionados con los recursos alojados en ese proveedor, se debe planificar y describir en el plan de empresa para respuesta ante incidentes.
- ✓ El ANS de cada proveedor de servicios *Cloud* debe garantizar el soporte en el manejo de incidentes necesario para la ejecución efectiva del plan de respuesta ante incidentes de la empresa en cada una de las etapas del proceso de gestión de incidentes: detección, análisis, contención, erradicación y recuperación.
- ✓ Las pruebas se llevarán a cabo al menos una vez al año. Los clientes deberían tratar de integrar sus procedimientos de pruebas con los de su proveedor (y otros socios) en la mayor medida posible. Lo ideal sería que un equipo (compuesto por miembros del cliente y del CSP) llevase a cabo varios ensayos de revisión de salud para un plan de respuesta ante incidentes y, como consecuencia, implementar las sugerencias en una nueva versión del plan de respuesta ante incidentes.

REFERENCIAS

- [1] GRANCE, T., KENT, K., and KIM, B. Computer Security Incident Handling Guide. NIST Special Publication 800-61.
- [2] MELL, P. and GRANCE, T. The NIST Definition of Cloud Computing, NIST Special Publication 800-145.
- [3] GROBAUER, B. and SCHRECK, T. October 2010. Towards Incident Handling in the Cloud: Challenges and Approaches. In Proceedings of the Third ACM Cloud Computing Security Workshop (CCSW), Chicago, Illinois.
- [4] WOLTHUSEN, S. 2009. Overcast: Forensic Discovery in Cloud Environments. In Proceedings of the Fifth International Conference on IT Security Incident Management and IT Forensics.

- [5] REED, J. 2011. Following Incidents into the Cloud. SANS Reading Room
- [6] DANYLIW, R., et al. 2007. The Incident Object Description Exchange Format, IETF Internet Draft RFC 5070.
- [7] MORIARTY, K. 2010. Real-time Inter-network Defense, IETF Internet Draft RFC 6045.
- [8] MORIARTY, K., and TRAMMELL, B. 2010. Transport of Real-time Inter-network Defense (RID) Messages, IETF Internet Draft RFC 6046.
- [9] FITZGERALD, E., et al. 2010. Common Event Expression (CEE) Overview. Report of the CEE Editorial Board.
- [10] BIRK, D. and WEGENER, C. 2011. Technical Issues of Forensic Investigations in Cloud Computing Environments In Proceedings of 6th International Workshop on Systematic Approaches to Digital Forensic Engineering (IEEE/SADFE), Oakland, CA, USA.

Dominio 10 //

SEGURIDAD DE APLICACIONES

Los entornos *Cloud*, particularmente los públicos, desafían muchos de los conceptos fundamentales de la seguridad de aplicaciones debido a su flexibilidad y transparencia. Aunque algunos de estos conceptos están bien entendidos, otros sin embargo no están tan claros. El objetivo de esta sección es proporcionar consejos acerca de la influencia que el *Cloud computing* tiene sobre el ciclo de vida de una aplicación, desde el diseño a la operación hasta su retirada final de servicio. Estos consejos están dirigidos a todas las partes interesadas (arquitectos de aplicaciones, profesionales de la seguridad, personal de operaciones y gestión técnica) y nos dan una visión sobre cómo reducir el riesgo y gestionar las garantías a la hora de diseñar aplicaciones de *Cloud computing*.

Cloud computing es un reto particular para aplicaciones que se desarrollan a lo largo de varias capas de *Software as a Service (SaaS)*, *Platform as a Service (PaaS)* o *Infrastructure as a Service (IaaS)*. Las aplicaciones de software basadas en *Cloud* requieren un rigor en el diseño similar a una aplicación que se conecta a Internet de forma directa – la seguridad debe ser facilitada por la propia aplicación sin suponer nada acerca de su entorno externo. Dado que las amenazas a las que están expuestas las aplicaciones de un entorno *cloud* son más numerosas que las que sufren aquellas en un CPD tradicional, la necesidad de seguir unas prácticas rigurosas cuando se desarrollan o se migran aplicaciones a *cloud* es mayor.

Introducción. El dominio de Seguridad de Aplicaciones se organiza en las siguientes áreas de interés:

- **SDLC⁵⁴ seguro:** Buenas prácticas para el ciclo de vida del desarrollo de software seguro junto con los matices específicos de un entorno Cloud.
- Autenticación, autorización, y cumplimiento legal - Arquitectura de seguridad de aplicaciones en Cloud.
- Identidad y el uso de identidad en su relación con la seguridad de aplicaciones en *Cloud*.
- Procesos de concesión de autorización y gestión de accesos basada en el riesgo y su relación con el cifrado en aplicaciones basadas en *Cloud*.
- Gestión de la autorización de las aplicaciones (creación de políticas, actualización, aplicación).
- Test de intrusión de aplicaciones *Cloud* (buenas prácticas junto con las peculiaridades de las aplicaciones basadas en *Cloud*).
- Monitorización de aplicaciones *Cloud*.
- Autenticación de aplicaciones, cumplimiento legal y gestión de riesgos y las repercusiones de la multipropiedad y la infraestructura compartida.
- La diferencia entre evitar software malicioso y proporcionar seguridad de aplicaciones.

10.1 SDLC (*Software Development Life Cycle/Ciclo de vida de Desarrollo de Software*) seguro

El concepto de Ciclo de Vida de Desarrollo del Software Seguro (SSDLC), también conocido por algunos como Ciclo de vida del Desarrollo Seguro o *Secure Development Life Cycle (SDLC)* es de gran importancia cuando se migran y despliegan aplicaciones en *cloud*. Las organizaciones deberían asegurar que las buenas prácticas de seguridad de aplicaciones, gestión de identidades, gestión de datos y privacidad son parte integral de sus programas de desarrollo a lo largo de todo el ciclo de vida de la aplicación.

⁵⁴ SDLC - *Software Development Life Cycle* – Ciclo de Vida de Desarrollo de Software

El desarrollo en un entorno *Cloud* difiere del desarrollo para entornos de alojamiento tradicionales en los siguientes aspectos:

- El control sobre la seguridad física se ve reducido sustancialmente en escenarios de *Cloud* pública.
- Las potenciales incompatibilidades que puedan existir entre proveedores (por ejemplo, en el almacenamiento) cuando se migran servicios de un proveedor a otro.
- La protección de los datos a lo largo de todo su ciclo de vida. Esto incluye tránsito, procesado y almacenamiento.
- Las combinaciones de servicios web en un entorno *Cloud*, que pueden potencialmente causar la aparición de nuevas vulnerabilidades.
- La dificultad de acceder a los *logs*, especialmente en un *Cloud* público compartido es más elevada, y debería de estar especificada como parte del acuerdo de nivel de servicio.
- La tolerancia a fallos (*fail-over*) para los datos y la seguridad de los mismos tiene que ser más detallada y estructurada en capas en un entorno *cloud* que en uno tradicional.
- Garantizar el cumplimiento legal (y tener pruebas que lo demuestren) de las normativas relevantes tanto de la industria como gubernamentales es habitualmente más difícil en un entorno *Cloud*.

Cuando se implementa un SSDLC, las organizaciones deben adoptar un conjunto de buenas prácticas de desarrollo. Este objetivo puede conseguirse realizando una correcta mezcla de de procesos, herramientas y tecnologías propias o adoptando alguno de los siguientes modelos de de madurez de software:

- *Building Security In Maturity Model (BSIMM2)*
- *Software Assurance Maturity Model (SAMM)*
- *Systems Security Engineering Capability Maturity Model (SSE-CMM)*

10.1.1 Programa de garantía de la seguridad de aplicaciones

Las organizaciones deberían de tener un programa de garantía de la seguridad de aplicaciones que asegure que las aplicaciones que van a ser migradas, desarrolladas o mantenidas en un entorno *Cloud* cumplen estos aspectos:

- Se tienen objetivos y métricas definidos, implementados, aprobados por la dirección y con un seguimiento adecuado.
- Se ha establecido una política de seguridad y privacidad para las aplicaciones en *cloud* que cumple los requisitos de cumplimiento legal alineados con las necesidades de negocio y las obligaciones de regulación de la organización.
- Se dispone dentro de la organización de la capacidad suficiente de garantía de la seguridad que permita la arquitectura, diseño, desarrollo, prueba y despliegue seguro de aplicaciones, pudiendo incorporar nuevos recursos y formarlos con una rapidez razonable.

- Se realizan evaluaciones del riesgo para la seguridad y la privacidad de todas las aplicaciones para asegurar que los requisitos están definidos correctamente.
- Se definen e implementan procesos para garantizar los requisitos de seguridad y privacidad durante los procesos de desarrollo y mantenimiento en el *Cloud*.
- Se deben poder auditar y verificar los procesos de gestión de la configuración y del cambio.
- Se realizan evaluaciones de los riesgos de seguridad física de las aplicaciones y sus datos, y se adecua el acceso de todos los componentes de la infraestructura *cloud* para cumplir los requisitos de seguridad.
- Se siguen durante la fase de desarrollo las mejores prácticas de programación formal, considerando las fortalezas y debilidades del lenguaje usado.
- Se deben de poder auditar y verificar las medidas de seguridad y privacidad.

10.1.2 Verificación y validación

10.1.2.1 Diseño

Cuando se especifican los requisitos de diseño específicos para una aplicación, hay que tener en cuenta que algunas funciones son más sensibles a la seguridad que otras, y que pueden no ser las mejores para ejecutarse en *Cloud*.

Se deberían seguir los siguientes principios para poder desarrollar un diseño seguro para una aplicación. Allí donde no se puedan cumplir estos principios con una arquitectura *cloud*, se deberán subsanar con los debidos controles técnicos y/o compensatorios. El no poder cumplir estos principios cuestiona la viabilidad de un despliegue *Cloud*.

- **Mínimo privilegio:** Este principio mantiene que una persona, proceso o entidad debería de tener acceso a los mínimos privilegios y recursos durante el mínimo periodo de tiempo requerido para realizar una tarea concreta. En muchos casos el mínimo privilegio solo puede ser implementado efectivamente a través de una gestión de la autorización de la aplicación contextual y granular, con mecanismos de políticas de seguridad automatizados⁵⁵.
- **Segregación de tareas:** Esta es una política de control que indica que ninguna persona debería de tener responsabilidades o acceso a dos o más funciones relacionadas una con la otra.
- **Defensa en profundidad:** La aplicación de varias capas de protección de modo que cada capa sigue ofreciendo seguridad en el caso de que la anterior haya sido comprometida.
- **Tolerancia a fallos:** Si un sistema *Cloud* falla, debería de hacerlo de forma que no comprometa la seguridad ni del sistema ni de los datos que contiene. Por ejemplo, una aplicación, en caso de fallo, puede denegar el acceso por defecto a todos los usuarios o procesos.
- **Economía de funcionamiento:** Se fomenta el uso de mecanismos de protección cuyo diseño e implementación sea sencillo y comprensible, de forma que no existan vías de acceso no intencionadas o éstas sean fácilmente identificables y eliminables.
- **Intercesión completa:** Toda petición de acceso realizada por cualquier entidad⁵⁶ para acceder un objeto de un sistema debe de ser autorizada.

⁵⁵ www.policyautomation.org

⁵⁶ Una entidad puede ser un usuario, código, un dispositivo, organización o agente.

- **Diseño abierto:** Un sistema *cloud* de acceso abierto que pueda ser evaluado y revisado por pares dentro de una comunidad de expertos tendrá un diseño más seguro.
- **Mínimo mecanismo común:** Se debería de emplear el mínimo de mecanismos comunes entre múltiples aplicaciones (especialmente los de protección), reduciendo la capacidad de una aplicación para corromper o afectar a otras.
- **Eslabón más débil:** Es importante identificar los mecanismos de seguridad más débiles dentro de una cadena de seguridad y sus capas de defensa y mejorarlos, de forma que el riesgo para el sistema pueda ser reducido a un nivel aceptable.

10.1.3 Construcción

10.1.3.1 Revisión de código

Se recomienda definir y seguir un proceso de desarrollo de software seguro a nivel de toda la organización. Pueden usarse a tal efecto las guías de prácticas básicas para el desarrollo de software seguro de SAFECODE⁵⁷, CERT (SEI)⁵⁸ o los estándares ISO.

El análisis dinámico examina el código de una aplicación *cloud* a medida que ésta se ejecuta, con el examinador enlazando los interfaces externos en el código fuente con las correspondientes interacciones en el código que se ejecuta. De esta forma las anomalías o vulnerabilidades que se observen en el código que está corriendo se pueden localizar a su vez en el código fuente y pueden ser corregidas.

A diferencia del análisis estático, el análisis dinámico facilita al examinador el probar el software en situaciones que puedan exponer vulnerabilidades debidas a la interacción con usuarios y cambios en la configuración o el comportamiento de otros componentes del entorno.

Se enumeran a continuación algunas de las mejores prácticas para escribir y revisar código seguro:

- Las aplicaciones *Cloud* deberían de tener la mínima información necesaria. Los comentarios deberían de ser eliminados del código en producción, y se debería de evitar incluir nombres y otro tipo de información personal.
- Se deberían usar herramientas de análisis del código fuente para comprobar que no tienen fallos típicos de programación como desbordamientos de buffer, ataques de formato de cadena, condiciones de carrera, etc.
- Verificar y validar todas las entradas, ya sean del usuario, del equipo o internas al sistema. La inyección de contenido y otros ataques son posibles si la infraestructura *cloud* acepta cualquier entrada y aplica su contenido directamente en comandos o sentencias SQL.
- Cuando se hace uso de código objeto (binarios), por ejemplo cuando se utilizan librerías de un tercero, emplear un servicio capaz de probar vulnerabilidades estáticas en dicho código.

⁵⁷ <http://www.safecode.org/>

⁵⁸ <https://www.cert.org/secure-coding/>

10.1.3.2 Pruebas de seguridad

Un test de intrusión o *pentest* es una metodología de pruebas de seguridad que ofrece al examinador una visión de la fortaleza de la seguridad de la red objetivo, simulando el ataque de un intruso empleando sus mismas tácticas y herramientas. El proceso implica un análisis activo del sistema *Cloud* en busca de cualquier vulnerabilidad potencial causada por una configuración pobre o deficiente del sistema, fallos conocidos y/o desconocidos del hardware/software y debilidades operacionales en los procesos o en las contramedidas técnicas. Este análisis se realiza desde la perspectiva de un atacante en potencia, y puede implicar la explotación activa de vulnerabilidades de seguridad.

El tipo de modelo de *Cloud* tiene una importancia tremenda a la hora de decidir si es posible o no realizar un test de intrusión. En general, en los modelos de *cloud Platform as a Service (PaaS)* e *Infrastructure as a Service (IaaS)* es bastante posible que los proveedores permitan los test de intrusión. Sin embargo en los modelos de *Software as a Service (SaaS)* es poco probable que los proveedores permitan a los clientes realizar test de intrusión sobre las aplicaciones y la infraestructura, con la posible excepción de terceras partes realizando un test de intrusión por encargo del propio proveedor de *Cloud* (en orden del cumplimiento legal o siguiendo buenas prácticas de seguridad).

Los test de intrusión se suelen realizar típicamente en un escenario de “caja negra”, es decir, sin un conocimiento previo de la infraestructura a probar. En su forma más sencilla, un test de intrusión se divide en tres fases:

1. **Preparación:** En esta fase se firma un contrato legal en el que especifica tanto la confidencialidad de datos del cliente como la protección legal del examinador. Como mínimo, se listan las direcciones IP que deberían de ser analizadas.
2. **Ejecución:** En esta fase se realiza el test de intrusión, en la que el examinador busca las posibles vulnerabilidades del sistema.
3. **Entrega:** Se comunican los resultados de la evaluación al contacto del examinador dentro de la organización, y se recomiendan las acciones correctivas correspondientes.

Tanto si el test de intrusión es con conocimiento total (caja blanca), conocimiento parcial (caja gris) o sin conocimiento alguno (caja negra), después de la obtención del informe y sus resultados, se tienen que aplicar técnicas de mitigación del riesgo hasta reducirlo a un nivel aceptable o tolerable. El test debería de tener un alcance lo más amplio posible a fin de cubrir las vulnerabilidad y los riesgos correspondientes en áreas como las aplicaciones, acceso remoto a sistemas y otros activos TIC relacionados.

10.1.3.3 Pruebas de interoperabilidad

Las pruebas de interoperabilidad evalúan si una aplicación *Cloud* puede intercambiar datos (interoperar) con otros componentes o aplicaciones. Estas pruebas determinan la capacidad de las aplicaciones para intercambiar datos a través de un conjunto común de formatos de intercambio, leer y escribir en dichos formatos y comunicarse empleando los mismos protocolos.

Uno de los principales objetivos de las pruebas de interoperabilidad es la detección de problemas entre distintas aplicaciones *Cloud* antes de que éstas sean puestas en producción. Para poder realizar las pruebas de interoperabilidad es necesario que gran parte de la aplicación esté terminada.

A la vez que se analiza la interoperabilidad, estas pruebas deberían confirmar que todos los intercambios de datos, protocolos e interfaces empleados están empleando medios seguros de transmisión de la información.

Las pruebas de interoperabilidad suelen tener típicamente tres aproximación:

1. **Probar todos los pares de dos en dos:** Esta prueba se realiza a veces por un grupo de examinadores independiente que conocen las características de interoperabilidad entre diversos productos de software y entre fabricantes de software.
2. **Probar una muestra de combinaciones:** Esta prueba consiste en probar solo una parte de las combinaciones posibles y asumir que si éstas funcionan correctamente el resto también interoperará de la misma forma.
3. **Probar contra una implementación de referencia:** Se establece una implementación de referencia (por ejemplo un estándar) y se prueban todos los productos contra esta referencia.

10.1.4 Mejora cuantitativa

10.1.4.1 Métricas

Todos los programas de garantía de la seguridad deberían de recopilar métricas que pueden ser analizadas y empleadas para informar de forma periódica del estado del desarrollo seguro. La colección de métricas e informes debería de ser incrementada a medida que el programa de seguridad de aplicaciones alcanza su madurez.

Algunas de las métricas recomendadas son:

- Porcentaje de aplicaciones y activos de datos en *Cloud* evaluados para su clasificación de riesgo en el último trimestre/año.
- Coste del programa de garantía de seguridad de aplicaciones en un trimestre/año dentro del coste trimestre/año del programa de las aplicaciones basadas en *Cloud*.
- Estimación de las pérdidas pasadas debidas a fallos de seguridad, si los hubiere, en las aplicaciones desarrolladas o desplegadas en *Cloud*.

10.1.4.2 Uso de herramientas y características de tecnologías de seguridad del SDLC automatizadas

Las actividades del SDLC centradas en personas (procesos, formación y pruebas) son necesarias pero a veces no son suficientes o viables para obtener una buena seguridad de aplicaciones. Donde sea posible, se deberían emplear herramientas automatizadas para construir aplicaciones seguras, así como incluir seguridad de forma automática dentro de las aplicaciones.

Estas herramientas que generan de forma automática características técnicas de seguridad en muchas ocasiones están ligadas a herramientas de desarrollo e integración/organización. Por ejemplo, se pueden generar automáticamente las reglas técnicas de una política de autorización (en tiempo de desarrollo e integración) a través de las especificaciones de seguridad de la aplicación empleando herramientas que analizan las aplicaciones y sus interacciones⁵⁹.

De forma similar, es posible realizar pruebas automatizadas en la fase de desarrollo e integración, generando a la vez evidencias de garantía de la seguridad de la información.

Dentro de un entorno *Cloud* puede realizarse desde el extremo del cliente durante el desarrollo (especialmente en IaaS), o el proveedor de puede proporcionarla (aunque el cliente tenga que adaptarla o configurarla), especialmente en un

⁵⁹ Este campo de la ciencia se denomina “model-driven security”, www.modeldrivensecurity.org

modelo PaaS. En los entornos SaaS lo más frecuente es que la automatización de la seguridad sea intrínseca a la aplicación, y que ésta sea configurada y operada por el proveedor de *cloud*.

10.2 Autenticación, autorización y cumplimiento legal – Arquitecturas de seguridad de aplicaciones en cloud

10.2.1 Desarrollo de servicios/aplicaciones cloud y retos de negocio

Cada día hay nuevos riesgos potenciales asociados con el acceso a sistemas y datos sensibles. El comprender claramente los siguientes riesgos de seguridad de un entorno de aplicaciones y de negocio es vital para tener una visión completa de las cuestiones de privacidad y seguridad dentro de los servicios y aplicaciones en *Cloud*:

- **Falta de control:** Se suele tener falta de control sobre los controles y políticas de seguridad *Cloud*.
- **Falta de visibilidad:** Se suele tener falta de visibilidad de la aplicación de las políticas de seguridad *Cloud* y de la efectividad de los controles.
- **Deficiencias en las capacidades de gestión:** Los clientes *Cloud* no suelen ser capaces de gestionar la seguridad de una aplicación *Cloud*, especialmente las políticas de acceso y auditoría.
- **Falta de Gobierno:** La organización no tiene control directo de la infraestructura; de ahí que la confianza (algunas veces ingenua) en el proveedor y en su capacidad de proporcionar la debida seguridad es primordial.
- **Riesgos de cumplimiento legal:** Dado que los sistemas y los datos están fuera del control directo de la organización, el proveedor *Cloud* puede afectar a la capacidad de la organización para cumplir con las normativas, expectativas de privacidad y estándares de la industria.
- **Fallos de aislamiento:** La multipropiedad y el uso de recursos compartidos son características que definen los entornos *Cloud*. Así pues, es perfectamente posible que compañías rivales estén usando los mismos servicios *Cloud*, ejecutando sus cargas de trabajo en el mismo equipo. Mantener el acceso a memoria, almacenamiento y red aislado es esencial en estos casos.
- **Protección de datos:** En algunos casos la organización cede el control directo sobre sus datos, recayendo en el proveedor el mantener éstos seguros, así como asegurar (o ser capaz de probar) que cuando se borran son eliminados permanentemente.
- **Interfaces de gestión y configuración de accesos:** Las aplicaciones *cloud* son accedidas y gestionadas a través de Internet, lo que potencialmente implica unos complejos requisitos de control. Así pues, se incrementa el riesgo asociado a una brecha de seguridad y toda autorización de acceso debería de ser considerada cuidadosamente.

10.2.2 Riesgos técnicos y soluciones

La mayoría de los proveedores de servicios *cloud* incluyen algún tipo de **IdEA**⁶⁰ (*Identity, Entitlement, and Access Management*, Identidad, Concesión de Derechos y Gestión de Acceso) dentro del diseño del servicio *Cloud*. En algunas ocasiones la autenticación y la autorización se delegan al sistema de gestión de usuarios del cliente mediante un estándar de federación.

El soporte de gestión de accesos, identidad y concesión de autorización afecta al cliente dado que la integración queda constreñida a las características del sistema de paso de credenciales. Otras infraestructuras como la medición y la facturación (que dependen de la gestión de identidades) también pueden presentar riesgos de integración y migración.

El soporte de gestión de accesos, identidad y concesión de autorización tiene implicaciones de integración para el cliente. Estas implicaciones incluyen el pasar de forma segura credenciales y atributos, aprovisionar usuarios adicionales, etc. Las operaciones de negocio dentro del proveedor de servicios *cloud* también se ven afectadas, incluyendo la facturación y contabilidad del uso de recursos. Como consecuencia, es importante el considerar la gestión de accesos, identidad y concesión de autorización como una parte integral del diseño.

Las capacidades de la aplicación a este respecto (o su falta), así como la capacidad de una aplicación de aceptar una afirmación **SAML**⁶¹, afectarán el Gobierno del servicio, la integración y la experiencia de usuario. Así pues, entender los requisitos de gestión de accesos, identidad y concesión de autorización de cada aplicación *cloud* particular es una parte crítica del proceso de definición de requisitos.

Son requisitos típicos de accesos, identidad y concesión de autorización de una aplicación *Cloud*:

- Comprender cómo la aplicación *cloud* aprovisionará cuentas de usuarios, usuarios avanzados y administradores - estos procesos pueden ser iniciados desde sistemas internos de RRHH o desde plataformas de RRHH en *Cloud*.
- La capacidad de aceptar peticiones y afirmaciones (identificadores y atributos) de una gran variedad de fuentes y entidades basadas en estándares de federación (por ejemplo *SAML*, *WS-Federation*, etc...)
- La capacidad de, basándose en el riesgo, realizar decisiones de concesión de autorización relativas al acceso a (y dentro de) la aplicación, teniendo en cuenta la identidad y atributos de todas las entidades de la cadena (usuarios, dispositivos, códigos, organizaciones y agentes).
- Un lenguaje de concesión de autorizaciones rico y basado en el riesgo, que conduzca a una gestión de accesos (creación, distribución, actualización, etc.) para todos los recursos protegidos (por ejemplo, qué está permitido para cada recurso).
- Soporte para los requisitos de cumplimiento legal para la seguridad interna y las políticas regulatorias, como autenticación basada en peticiones o controles de acceso basados en roles de mínimos.
- Monitorización de actividad de usuarios, *logging* e informes dictados por políticas internas y cumplimiento de normativas como SOX, PCI e HIPAA.

⁶⁰ **IdEA** - *Identity, Entitlement, and Access Management* o Gestión de Derechos, Identidad y Concesión de Autorización.

⁶¹ **SAML** - *Security Assertion Markup Language*, (Lenguaje de Marcas de Afirmaciones de Seguridad), un estándar abierto basado en XML para el intercambio de datos de autenticación y autorización entre dominios de seguridad desarrollado por OASIS.

Una variedad de proveedores de identidad o de servicio pueden generar tokens (*SAML*, *OpenID*⁶², o *OAuth*⁶³) para la caché de sesiones, permitiendo capacidades de traspaso de inicio de sesión (*pass-through sign-on capability*). Las aplicaciones a desplegar en el *cloud* deberían de ser capaces de integrarse con estos servicios de petición/afirmación, y las aplicaciones y servicios deberían de ser diseñadas para soportar estándares abiertos de federación como SAML, OAuth y OpenID.

El proceso de gestión de concesión de autorizaciones deberá tener la capacidad de definir, gestionar y acceder las reglas de control de acceso para las aplicaciones basadas en *cloud* a través de un interface centralizado. Dicho interface/servicio puede estar albergado en el *cloud* o internamente, y puede apoyarse en estándares como **XACML**⁶⁴. El reto principal es la gestionabilidad: Con el incremento de la complejidad de las políticas de seguridad, el cumplimiento legal y las tecnologías, la tarea de traducir las políticas de seguridad a una implementación final se hace más costosa en tiempo y recursos, repetitiva y propensa a errores. Esto puede terminar sumando la mayor parte de los costes de seguridad para las organizaciones finales, ya que se tiene que gestionar la entrada y salida de los usuarios en listas de acceso basadas en roles, todo ello mientras procesos muy costosos vigilan estas listas y aseguran que no se incumple la separación de deberes.

<i>Petición / Atributo</i>	Acceso corporativo de directivos de RRHH	Acceso corporativo de usuarios	Acceso de directivos de RRHH desde casa (portátil corporativo)	Acceso de usuarios desde casa (dispositivo propio)
ID: Organización	Válido	Válido	Válido	No
ID: Identificador de usuario	Válido	Válido	Válido	Válido
ID: Dispositivo	Válido	Válido	Válido	No
Atrib: Dispositivo limpio	Válido	Válido	Válido	Desconocido
Atrib: Dispositivo parcheado	Válido	Válido	Válido	Desconocido
Atrib: IP del dispositivo (¿está en la red corporative?)	Válido	Válido	No	No
Atrib: Usuario es directivo de RRHH	Válido	No	Válido	No
Resultado del acceso	Acceso de lectura/escritura a todas las cuentas de RRHH	Acceso lectura/escritura a la cuenta de RRHH del usuario	Acceso lectura/escritura a las cuentas de RRHH de usuarios	Acceso de lectura a la cuenta de RRHH del usuario

Tabla 7 - Ejemplo de matriz de concesión de autorizaciones para una aplicación cloud de RRHH

Definir en su lugar un conjunto de reglas dentro de una capa de concesión de autorizaciones, alimentada por las peticiones (afirmaciones) y atributos de las entidades de la transacción simplifica de forma significativa y aumenta el control que se tiene sobre las aplicaciones, conduciendo a un menor coste para las organizaciones finales (y de los proveedores *Cloud*) y una mejora de la precisión de la implementación de políticas.

⁶² **OpenID** – Un estándar abierto que permite que los usuarios se autenticuen de forma descentralizada

⁶³ **OAuth** - Open Authorization (Autorización Abierta), un estándar abierto para la autorización que permite a los usuarios compartir recursos privados mediante tokens en lugar de credenciales.

⁶⁴ **XACML**- eXtensible Access Control Markup Language (Lenguaje de marcas para el control extensible de accesos), un estándar OASIS

Para integrar controles de seguridad, seguridad de datos y protección de la privacidad, los servicios deberían de usar estándares de la industria auditables como ISAE 3402/SSAE 16 (substituye a SAS 70), PCI, HIPAA o ISO 27002. Cada uno de ellos viene con una serie de controles ordenados por categorías que gobiernan tanto la operación de un CPD como la de las aplicaciones que pueden ser albergadas en dicho entorno.

Es importante evaluar las distintas demandas de seguridad y hacer una decisión responsable sobre qué estándares se aplican a las aplicaciones y servicios albergados en un entorno *Cloud*. Se debería de llevar a cabo un análisis meticuloso basado en los requisitos de seguridad para identificar por adelantado los objetivos de nivel de servicio. De esta forma los clientes y los proveedores de *Cloud* se podrán evitar cambios profundos en el código de la aplicación, su despliegue y las herramientas de soporte.

10.2.3 Fundamentos del cumplimiento legal

Independientemente de los estándares usados, el conseguir el cumplimiento legal a la hora de ejecutar una aplicación en el *Cloud* tiene varios pilares, siendo la base de todos ellos la infraestructura física proporcionada por el proveedor de *Cloud*. Los controles de la infraestructura física incluyen entre otros aspectos cómo proteger las instalaciones de desastres naturales, garantizar el suministro eléctrico durante apagones y hacer copias de seguridad de los datos en caso de un fallo de hardware. También incluyen controles que rigen las políticas y procesos del proveedor de *Cloud* como auditoría administrativa de los sistemas, acceso y autorización al CPD y métodos empleados en la revisión de la seguridad interna, junto con cómo éstos se comportan e informan.

La siguiente capa por encima de los controles de la infraestructura consiste en una serie de controles de aplicación. Se requieren múltiples niveles de seguridad, empezando con que la capa de transporte sea segura; cuando los datos dejan el CPD, deben de estar cifrados con claves bajo el control de la empresa. Algunas aplicaciones pueden necesitar una capa de seguridad de mensajes, firmas digitales y otras medidas de seguridad añadidas para poder cumplir con algunos estándares de almacenamiento y transmisión de información de datos personales necesarios para cumplir requisitos de privacidad. Todos estos controles de la aplicación o servicio que va a ser migrada al *Cloud* deberían de ser identificados durante la fase de diseño, para que así puedan ser integrados de forma apropiada en el diseño de la arquitectura y desarrollados según sus requerimientos. Los estándares de cumplimiento legal más conocidos son *PCI –DSS*, *SOX*, *ISAE 3402/SSAE 16*, *HIPAA* y otros estándares de privacidad.

10.3 Identidad, concesión de autorizaciones y gestión de accesos para la seguridad de aplicaciones *Cloud*

Las aplicaciones desarrolladas de forma interna se protegen con controles de seguridad perimetral tradicionales como cortafuegos, proxis, etc. De esta forma se pueden alcanzar los niveles de riesgo y los requisitos de seguridad deseados por la empresa, ya que las aplicaciones se ejecutan en redes confiables, hardware confiable, etc. La empresa puede también apoyarse en su infraestructura de directorio para autenticar a los usuarios en esas aplicaciones y mantener todas las decisiones de acceso dentro de las mismas. El perímetro de seguridad de la empresa está perfectamente definido en este caso.

Cuando el usuario migra estas aplicaciones al *Cloud*, todos estos controles tradicionales dejan de ser lo suficientemente efectivos como para proteger las aplicaciones, ya que estas se ejecutan en redes no confiables (desparametrización). Las aplicaciones del cliente pueden cohabitar con otros clientes del proveedor de servicios (*pool* de recursos) y pueden ser

accedidas desde cualquier parte empleando cualquier tipo de dispositivo. Esto cambia la verdadera naturaleza de los requisitos de seguridad para las aplicaciones *Cloud*. Tal y como se indica en www.rationalsurvivability.com la anatomía de un *Cloud* se remite a la siguiente estructura:



Figura 11 – Anatomía de un Cloud

A esta estructura el usuario puede añadir ahora las formas a través de las que se puede acceder a las aplicaciones. Esta anatomía puede ser vista como:



Figura 12—Componentes de entrega de un Cloud

En la anatomía anterior se puede ver claramente que la aplicación es una ventana a los datos, y que el nuevo perímetro es el contenido (los datos) y el contexto a través del cual el usuario intenta acceder al mismo. Esto hace que aplicar controles de seguridad a las aplicaciones *Cloud* sea crítico. El contexto bajo el que se accede a los datos se convierte en algo muy importante que necesita una colección abundante de identificadores y atributos con los que tomar decisiones de acceso. Con el auge las tecnologías TIC orientadas al consumidor, las empresas se enfrentan con la realidad del BYOD (*Bring Your Own Device* o Trae Tu Propio Dispositivo). Es por ello que la identificación del dispositivo y los atributos del mismo se convierten en factores importantes a la hora de determinar el control de accesos.

La identidad no debería de ser vista como una referencia para la autenticación de la entidad sino como un medio para recoger más información del usuario para tomar decisiones de acceso. Dentro de la identidad también incluimos las identidades de los dispositivos en los que se ejecutan las aplicaciones (por ejemplo, la identidad de una imagen de una

máquina virtual o VM), los usuarios con privilegios para gestionar esa imagen de VM (que podrían ser tanto usuarios de la empresa como del proveedor de servicios), identidades de otras aplicaciones y servicios con los que la aplicación tiene que interactuar, identidades de los usuarios administradores que gestionan la aplicación y entidades externas a la empresa que necesitan acceso a la aplicación como B2B, B2C, etc.

También hay que tener en cuenta que las decisiones de acceso estarán basadas en atributos que no están relacionados con la identidad, y que las herramientas de creación/gestión de políticas tienen que dar soporte a dichos atributos (ver “Gestión de la autorización & Automatización de políticas” más abajo).

En esta sección nos fijaremos en cómo la identidad, la concesión de autorización y la gestión de accesos afecta a la seguridad de aplicaciones *Cloud*. El IdEA (*Identity, Entitlement, and Access Management*) puede ser dividido en términos generales en cinco componentes principales:

1. Autenticación.
2. Autorización.
3. Administración.
4. Auditoría y cumplimiento legal.
5. Políticas.

10.3.1 Autenticación

La autenticación se refiere a la capacidad de establecer/afirmar una identidad a una aplicación. Habitualmente esto se hace en dos fases: la primera fase es desambiguar la identidad, y la segunda es validar las credenciales facilitadas al usuario. Algunos de los principales aspectos de la autenticación de aplicaciones *Cloud* son la independencia de dispositivos, las interfaces gráficas simples y comunes y el uso de protocolos únicos y universales entre los dispositivos. De la misma forma, muchos proveedores de servicios ofrecen sus servicios en forma de **APIs**, y estas APIs se diseñan para que acepten tokens en lugar de las contraseñas.

La autenticación en una aplicación empresarial tradicional se realiza contra el almacén corporativo de usuarios (*Active Directory* o LDAP), y las credenciales de autenticación son habitualmente usuario/contraseña. En aplicaciones basadas en *Cloud* la autenticación se vuelve algo más complicada. Algunas empresas establecen túneles VPN desde el proveedor de servicios hasta la red de la empresa de modo que pueden autenticarse contra el almacén corporativo de usuarios. Aunque pueda ser válida, la empresa tendría que tener en cuenta temas de latencia, conectividad, planes de continuidad de negocio (BCP) y recuperación ante desastres (DR), etc., por lo que esta solución no debería de ser usada o diseñada para nuevas aplicaciones *Cloud*. Las empresas deberían plantearse el uso de estándares abiertos como *SAML* y *WS-Federation*.

El uso de las aplicaciones de la empresa por parte de socios y clientes suele incrementarse hoy en día, lo que también se cumple en las aplicaciones *Cloud*. Estos usuarios raras veces quieren tener identidades separadas para su acceso como terceros (pero hoy en día a veces no tienen otra opción). Las empresas deberían planear el BYOI (*Bring Your Own Identity*, Trae Tu Propia Identidad), estando las aplicaciones diseñadas para consumir identidades y atributos de múltiples organizaciones.

Desde que las aplicaciones *Cloud* son ampliamente accesibles a través de varios dispositivos, la autenticación con simples usuarios y contraseñas debería ser dejada de tener en cuenta como una solución. Las empresas deberían planear emplear una autenticación más fuerte, y los clientes deberían de considerar una autenticación fuerte para la confirmación de la identidad original, determinando el tipo de credenciales que cumpla su requisito de riesgo (*token* RSA, OTP sobre SMS o teléfono, Smartcard/PKI, biometría, etc.). Esta confirmación permitiría que los identificadores y atributos fueran pasados a la aplicación *Cloud* con un fuerte nivel de autenticación, de forma que la capa de concesión de autorizaciones podría realizar decisiones mejores basadas en el riesgo para la gestión de accesos.

Las empresas deberían preparar una autenticación basada en riesgos para sus aplicaciones *Cloud*. Este tipo de autenticación está basada en factores como el identificador del dispositivo, geolocalización, proveedor de servicios de Internet, información heurística, etc. Las aplicaciones *Cloud* no deberían de realizar una autenticación únicamente durante la conexión inicial, sino que deberían de proceder a la autenticación basada en riesgos en función de las transacciones que realiza la aplicación.

Las aplicaciones *Cloud* deberían de apoyarse en estándares como SAML y OAuth cuando fuera aplicable. Como se ha mencionado con anterioridad, las APIs de un servicio *Cloud* están diseñadas para aceptar *tokens* y no contraseñas, por lo que un usuario que intente acceder a servicios *Cloud* desde su dispositivo móvil tiene primero que autenticarse contra su proveedor de identidad (hoy en día probablemente su empresa), y una afirmación SAML se genera y se pasa al proveedor de servicios *Cloud*. Una vez validada con éxito la afirmación SAML, se genera un *token* OAuth y se transfiere al dispositivo móvil. Éste pasa los *tokens* a los servicios de acceso *Cloud* (usualmente APIs basadas en REST⁶⁵).

10.3.2 Autorización y control de accesos

La autorización en su término más amplio se refiere al cumplimiento de las reglas por las cuales se otorga acceso a los recursos. El proceso de concesión de autorización implementa políticas de negocio que se traducen en acceso a los recursos de la empresa. En las aplicaciones basadas en *Cloud* la autorización no debería de realizarse únicamente por el contenido sino también por el contexto.

En un modelo de autorización centrado en el usuario, éste se convierte en el PDP⁶⁶. El usuario determina el acceso a sus recursos y el proveedor de servicios *Cloud* actúa como un PEP⁶⁷. OAuth es usado ampliamente en este modelo, aunque UMA (*User Managed Access* o Acceso Gestionado por el Usuario) es también un estándar emergente en esta área.

En un modelo de autorización centrado en la empresa, la empresa es el PDP o PAP⁶⁸, y el proveedor de servicios actúa como PEP. En algunos casos las empresas implementan portales de seguridad *Cloud* para PEP. La empresa cliente debería considerar el uso de XACML y la gestión centralizada de políticas.

Las aplicaciones *Cloud* pueden apoyarse en múltiples tipos de servicios. Algunos servicios pueden ser aplicaciones *legacy* que se ofrecen como servicios web a través de *middleware*, o pueden ser servicios web nativos del *Cloud*. La diversidad de la cadena de suministro de entrega, aunque abstraída por el interface de servicios web, puede complicar el proceso de Gobierno.

⁶⁵ REST - Representational state transfer, un estilo de arquitectura de software para sistemas hipermedia distribuidos.

⁶⁶ PDP - *Policy Decision Point* o Punto de Decisión de la Política.

⁶⁷ PEP - *Policy Enforcement Point* o Punto de Cumplimiento de la Política.

⁶⁸ PAP - *Policy Access Point* o Punto de Acceso de la Política.

El Gobierno, en tiempo de diseño, engloba definir, desarrollar y registrar los servicios, así como implementar los requisitos de políticas para acceder a los mismos. El Gobierno, en tiempo de ejecución, engloba localizar los servicios, implementar restricciones de seguridad para su invocación, imponer restricciones de seguridad para el acceso y auditar todos los accesos. Se recomienda usar estándares abiertos como W3C **WS-policy**⁶⁹ para definir las afirmaciones para las políticas de gestión y seguridad, WS-security para el cumplimiento de las restricciones de acceso, WS-trust para implementar **STS**⁷⁰ (*Secure Token Service*, Servicio de Tokens Seguro) y así generar tokens e intercambiar formatos de token, etc.

Existen diferentes tipos de modelos de autorización: Basados en roles, basados en reglas, basados en atributos, basados en peticiones y basados en autorización como **ZBAC**⁷¹. Las empresas que ya posean su propia solución **WAM**⁷² deberían apoyarse en ésta para proteger a su vez las aplicaciones *Cloud*. La mayoría de los productos WAM soportan controles de acceso basados en roles y en reglas.

Los arquitectos de aplicaciones y los diseñadores deberían planear una migración a sistemas basados en reglas, empleando peticiones y atributos como fuente de dichas reglas a través del proceso de concesión de autorización descrito arriba en detrimento de otras soluciones *legacy*.

Cuando se hace uso de control de acceso basado en atributos, el **IdP**⁷³ pasa los atributos al proveedor de servicios *Cloud* para su aplicación. Los proveedores de identidad deberían tener en cuenta que:

- Los atributos adjuntados a la identidad no tienen que referirse de forma estricta a la identidad (como nombre, apellidos, dirección de correo electrónico, etc.). También pueden incluir direcciones IP, información de localización, afiliación a un grupo, número de teléfono, etc.
- Debe de tenerse cuidado a la hora de compartir atributos que identifican directamente al usuario a causa de las posibles cuestiones de privacidad.
- Las empresas deberían tener en cuenta la complejidad de los atributos a la hora de tomar decisiones de control de accesos. Deberían de saber qué proveedor de atributos tienen que contactar para una autorización particular basada en atributos, y saber en qué agregadores de atributos pueden apoyarse (aunque éstos pueden simplificar o complicar la confianza). También deberían de tener en consideración las complejidades de la resolución de conflictos, el manejo de datos incompletos, etc.
- Se debería considerar también la extensibilidad de los atributos: validación (verificabilidad), condiciones de uso, fecha, etc.
- Las empresas deberían de considerar la privacidad, las ARP (*attribute release policies* o políticas de cesión de atributos) y el consentimiento. Algunos ejemplos pueden ser las directivas de privacidad de la UE, leyes locales y estatales, etc. La localización del proveedor de identidad y del proveedor de servicios *Cloud* es un factor importante a este respecto.
- Se debería de ceder la información mínima necesaria para el control de acceso.

⁶⁹ **WS** - *Web Service* o Servicio Web

⁷⁰ **STS** - *Secure Token Service* o Servicio de Token Seguro

⁷¹ Descrito en publicaciones por Alan Karp, HP Labs

⁷² **WAM** - *Web Access Management* o Gestión de Acceso Web

⁷³ **IdP** - *Identity Provider* o Proveedor de Identidad

- Las empresas deberían asegurar el soporte de atributos no centrados en la identidad.
- Se debería garantizar por parte de las empresas que las políticas de acceso y concesión de autorización son gestionables a la par que su aplicación es técnicamente posible. El uso de tecnologías de automatización de políticas puede ser una posible solución (posiblemente enlazadas con las herramientas de la propia aplicación PaaS).

El objetivo principal del control de acceso basado en peticiones es compartir la información de forma controlada, ya que las peticiones se basan en el contexto de la transacción. Cuando se plantea el uso de la autorización basada en peticiones, una empresa debería de considerar a su vez:

- El uso de peticiones significativas (direcciones de correo electrónico verificadas en lugar de simples direcciones de correo electrónico).
- Tipo, garantía, antigüedad y calidad de la petición (si la petición se cachea fuera del proveedor de peticiones en este caso se pierde la frescura de la petición).
- La autoridad correcta de las peticiones basadas en el contexto. Por ejemplo, una compañía de telecomunicaciones tiene autoridad para verificar un número de teléfono de un cliente, un proveedor de correo para verificar una dirección de correo, etc.
- Usar intermediaciones (*brokers*) de peticiones donde sea posible, ya que pueden ser usados para abstraer varios proveedores de peticiones (por ejemplo, podrían crear un paquete de peticiones a un nivel de confianza deseado y crear un punto central para los permisos de usuarios).
- Ceder la mínima parte de la petición necesaria para la transacción.

La aplicación *Cloud* puede ser también una mezcla de varias aplicaciones *Cloud* (*mash-up*) corriendo en el mismo o diferentes proveedores de servicio. La empresa debería de planear como se autentican los usuarios de forma transparente en todas estas aplicaciones, y cómo se comparten los perfiles de usuarios (pertenencia a grupos, concesiones de autorización, roles, etc.) a lo largo de las mismas para poder realizar controles de acceso granulares. Se recomienda el uso en este caso de estándares abiertos (SAML, OAuth, XACML, etc.).

10.3.3 Administración y gestión

EIDM⁷⁴ dentro de una empresa está enfocada principalmente a la gestión de usuarios (aprovisionamiento) y en la gestión de políticas de acceso (a las aplicaciones de la empresa). IDM es un componente muy importante de IdEA, no solo porque ofrece un acceso rápido a los usuarios sino porque permite una pronta revocación del acceso y una rápida gestión del acceso en caso de que el usuario cambie a un rol diferente.

La gestión de identidad se suele integrar firmemente y está conectada directamente con los almacenes de datos (usuarios, políticas, etc.). En muchos despliegues suele estar fuertemente personalizada. Debido a la naturaleza distribuida de las aplicaciones *Cloud* no es posible aplicar el mismo principio, ya que la IDM puede no tener acceso directo a los almacenes de datos en el proveedor de servicios. Además, no hay una API estándar para el

⁷⁴ IDM - Identity Management o Gestión de Identidades

aprovisionamiento ya que muchos proveedores de servicio no han adoptado **SPML**⁷⁵ (*Service Provisioning Mark-up Language* o Lenguaje de Marcas de Aprovisionamiento de Servicios).

La IDM en el contexto *Cloud* no debería gestionar únicamente las identidades de los usuarios. Debería extenderse para gestionar las identidades de aplicaciones y servicios, sus políticas de control de accesos, las identidades con privilegios, etc.

El aprovisionamiento federado actualmente se implementa mediante APIs ofrecidas por el proveedor de servicios. El modelo PUSH seguido por una IDM corporativa no funcionará con aplicaciones *Cloud* ya que puede sobrecargar los proveedores de servicios.

El estándar emergente en la actualidad es **SCIM**⁷⁶, cuyo objetivo principal es hacer más barata la gestión de identidades, con una implementación más barata y rápida. El objetivo secundario es facilitar la migración de identidades de usuario dentro y fuera del *Cloud*. SCIM es sencillo porque usa un esquema central bien definido, amigable con *Cloud* ya que usa APIs REST soportadas por muchos proveedores de servicios *Cloud*, y soporta gestión de identidades porque trabaja con protocolos ya existentes como SAML, OpenID, etc. Basándonos en estos hechos (a la hora de escribir este documento) SCIM podría ser adoptado como un estándar de la industria para aprovisionamiento de identidades.

Algunos de los retos considerados por las empresas relativos a la gestión de identidades son:

- Como sincronizar cambios de las identidades o accesos entre empresa → *Cloud*, *Cloud* → *Cloud* y *Cloud* → empresa.
- Como desaproveccionar identidades y accesos a lo largo de la empresa y *Cloud*.
- Como crear, actualizar y gestionar políticas de acceso de una forma gestionable, escalable, barata y de bajo mantenimiento.

La solución actual para muchas empresas es la adopción de una solución IDM híbrida que abarca tanto a la empresa como al CSP.

La gestión de políticas de acceso es uno de los retos principales de la seguridad de aplicaciones, siendo a menudo la solución la automatización de seguridad: la automatización de las políticas de seguridad es especialmente importante en *Cloud* debido a que los usuarios *Cloud* demandarán a los CSP el soporte de gestión de políticas de cumplimiento legal y regulatorio. Al mismo tiempo se juzgará el ROI (Retorno de Inversión) con el mismo rasero aplicado a *Cloud* en general, es decir, la medida en la que reducen sus costes iniciales de capital y su coste de mantenimiento interno anual.

10.3.4 Auditoría/Cumplimiento legal

Las empresas que usan servicios *Cloud* deberían hacerse tres preguntas fundamentales:

1. ¿A qué recursos *Cloud* tiene acceso un usuario?
2. ¿Qué recursos emplea realmente el usuario?

⁷⁵ SPML - *Service Provisioning Mark-up Language* – Lenguaje de Marcas para el Aprovisionamiento de Servicio

⁷⁶ SCIM - *Simple Cloud Identity Management* – Gestión Simple de Identidad Cloud

3. ¿Qué reglas de política de acceso fueron usadas como base para tomar una decisión?

Con los despliegues *Cloud* actuales, los clientes empresariales tienen una visibilidad muy limitada de los datos de auditoría de los proveedores de servicios *Cloud*. Una empresa necesita acceso a esta información no solo para el cumplimiento legal impuesto por el negocio, sino para cumplir las regulaciones de la industria y tratar con las disputas de fraude.

El mercado de IDM se mueve en la actualidad hacia el **IAG**⁷⁷. Las empresas deberían considerar también el uso de herramientas SIEM (*Security Incident & Event Management* o Gestión de Eventos e Incidentes de Seguridad) para correlar los datos de registros de acceso a las aplicaciones *Cloud* y los datos de la política de acceso para generar informes de cumplimiento de la política, así como el uso de estándares de la industria auditables como ISAE 3402/SSAE 16, HIPPA, DSS PCI, ISO27002, etc.

Las consideraciones generales de IdEA para la seguridad de aplicaciones *Cloud* son:

- La identidad, la concesión de autorización y la gestión de accesos no deberían implantarse en el último momento; deberían más bien ser integradas dentro del SDLC de una aplicación, empezando con la recogida de requisitos.
- Durante la fase de diseño se debe considerar cómo controlar el acceso a la aplicación empleando un acceso basado en peticiones siempre que sea posible.
- Se debe considerar emplear herramientas como SAPM (*Shared Account Password Management* o Gestión de Contraseñas de Cuentas Compartidas) para gestionar cuentas con privilegios elevados dentro de la aplicación. Así se posibilita la segregación de tareas y el mínimo privilegio.
- Si la empresa ya tiene herramientas de gestión de acceso web, debe asegurarse que estas herramientas pueden extenderse a entornos *Cloud* (por ejemplo, añadiendo capacidades SAML).
- Las aplicaciones *Cloud* pueden necesitar apoyarse en servicios ofrecidos por proveedores como *logging*, conectividad a bases de datos, etc. Muchos de estos proveedores exponen estos servicios a través de APIs o servicios web. El acceso a estos servicios podría estar controlado por *tokens* OAuth. Las aplicaciones *Cloud* deberían tener en cuenta el soporte de varios tipos de *token* como OAuth, claves API, etc.
- Se debe asegurar que se sigue un proceso de desarrollo ágil y que la aplicación se construye en componentes modulares. De esta forma la aplicación puede hacer uso de estándares emergentes en un futuro como el *browserID* de Mozilla, *U-Prove* de Microsoft o *UMA* de la Iniciativa Kantara.

Es necesario ser consciente de las amenazas a las aplicaciones *Cloud*, que incluyen:

- **Spoofing.** Falsificar la identidad de otro usuario.
- **Manipulación.** Modificar los datos en tránsito.
- **Repudiación.** Denegar el origen de una transacción (petición o respuesta).
- **Revelación de información.** Revelar datos sin tener autorización.

⁷⁷ **IAG** – *Identity and Access Governance* o Gobierno? de la Identidad y el Acceso

- **Denegación de servicio.** Afectar a la disponibilidad.
- **Escalada de privilegios.** Asumir un rol o concesión de autorización.

Estas amenazas podrían tratarse con IdEA de la forma siguiente:

- **Spoofing.** Autenticación fuerte.
- **Manipulación.** Firmas digitales o *hash* (como se usan en las afirmaciones SAML).
- **Repudiación.** Firmas digitales (como se usan en las afirmaciones SAML), registros de auditoría.
- **Revelación de Información.** SSL, cifrado (no específicamente estricto de IdEA).
- **Denegación de servicio.** Portales de seguridad (Portales de seguridad de servicios web).
- **Escalada de privilegios.** Autorización (OAuth).

10.3.5 Gestión de políticas

La gestión de políticas de acceso (a menudo llamada “gestión de la autorización” si se realiza centrada en las concesiones de autorización) es el proceso de especificar y mantener políticas de acceso a los recursos, basándose en atributos: relacionados con el origen (por ejemplo, autenticación de origen), el contexto (entorno, negocio o TIC) o el destino (regulación de acceso o políticas de QoS⁷⁸).

La gestión de la concesión de autorizaciones forma parte de la gestión de acceso y autorización, que incluye crear y mantener políticas para atributos que no están relacionados directamente con la identidad pero que son necesarios (además de la identidad y sus atributos) para hacer una decisión de acceso coherente.

La concesión de autorizaciones/autorización también tiene en cuenta atributos que no están relacionados con una identidad, por ejemplo:

- Estado general del paisaje TIC, procesos de negocio a negocio, interconexión de sistemas TIC o procesos de negocio, el entorno, etc. (por ejemplo, nivel de una crisis, situaciones de emergencia).
- Otras decisiones realizadas por otras entidades (por ejemplo, vistos buenos, decisiones previas).
- Atributos relacionados con el recurso protegido objetivo (por ejemplo, QoS o políticas de regulación de acceso).

La gestión de la autorización, la toma de decisiones y el proceso de aplicación se realiza típicamente de una de estas tres formas:

1. Usando un punto de aplicación de la política central o externo / Servidor de políticas / Política como Servicio.
2. Embebida como parte de la aplicación *Cloud*.
3. Usando una Identidad como Servicio o Persona como Servicio (una entidad Persona se define como su identidad y un conjunto de atributos seleccionados).

⁷⁸ Lang, U. “Access Policies for Middleware”, PhD thesis, University of Cambridge Computer Laboratory, 2003

10.3.5.1 Cuestiones del Cloud vs. Gestión de políticas

La gestión de autorización/concesión de autorizaciones en el *Cloud* se enfrenta a varias cuestiones⁷⁹.

En primer lugar, la gestión de la concesión de autorizaciones en el *Cloud* tiene el problema concreto que los clientes de *Cloud* a menudo no tienen suficiente control sobre la toma de decisiones técnicas sobre políticas de acceso (y su aplicación) en la infraestructura *Cloud*. Hoy en día, muchos CSP no ofrecen puntos de aplicación de políticas configurables por el cliente (por ejemplo, basados en el estándar XACML de OASIS), y los proveedores de *Cloud* no pueden preconfigurar políticas específicas para los clientes por ellos (porque obviamente, es algo que debe hacer cada cliente).

En segundo lugar, una complejidad de la gestión de concesión de autorizaciones para *Cloud* interconectadas (mash-ups) es que el acceso tiene que estar controlado para toda las *Cloud* interconectadas, no solo para cada *Cloud* individual. Esto significa que todas las políticas tienen que ser creadas teniendo en mente el uso de cadenas de servicio y delegación a lo largo de las *Cloud* interconectadas.

10.3.5.2 Buenas prácticas para la gestión de la autorización

- Establecer cuándo una perspectiva centrada en la identidad y la concesión de autorizaciones es la mejor vía para crear y gestionar las políticas de acceso en la organización; en muchos casos una perspectiva centrada en la protección de recursos puede ser más fácil de crear y mantener porque a menudo el objetivo final es proteger dichos recursos, y las políticas a menudo se distribuyen a los sistemas protegidos finales para su aplicación automática (por ejemplo, en sistemas de gestión de la concesión de autorizaciones / autorización). En estos casos la identidad es meramente un atributo en una política de acceso que se escribe con el objetivo del cumplimiento en el sistema protegido final en mente.
- Tener seguridad de que las políticas están especificadas de forma gestionable. Incluye especificar políticas que sean genéricas, especificadas con un nivel suficientemente alto de abstracción, y expresadas de forma clara para su entendimiento por parte de las personas/negocios/organizaciones relevantes. Existen mecanismos y herramientas para generar las reglas técnicas detalladas de las políticas de acceso a través de dichas políticas gestionables (por ejemplo, empleando la automatización de las políticas de seguridad dirigidas por modelos).

10.3.5.3 Arquitecturas de *interface* con proveedores de políticas de acceso

Los puntos de decisión/aplicación de políticas (PEPs/PDPs) que emplean protocolos estándar (por ejemplo, XACML) o propietarios (servicios web directos u otras llamadas mediante *middleware*) pueden acceder a servidores de políticas de acceso (que contienen las reglas de un *mash-up cloud* interconectado). La arquitectura es habitualmente un servidor para varios PDPs/PEPs si la política cubre un solo dominio de confianza (por ejemplo, la intranet de una empresa).

Sin embargo, en despliegues de mayor envergadura se pueden tener varios servidores de políticas federados que sirven a múltiples PDPs/PEPs diferentes. Existen varios productos de gestión de accesos que soportan reglas de gestión de la autorización (por ejemplo, en XACML) que pueden ser usados para expresar concesiones de autorización para identidades. De la misma forma, existen varios productos que pueden ser usados para crear políticas de autorización desde una perspectiva más centrada en los recursos objetivos.

⁷⁹ Details: Lang U, Schreiner R, Analysis of recommended cloud security controls to validate OpenPMF, Information Security Technical Report (2011), doi:10.1016/j.istr.2011.08.001

10.3.5.4 Aprovisionamiento de políticas de acceso

Además del aprovisionamiento de identidades y atributos, las políticas de acceso también deben de ser aprovisionadas (ver el punto anterior). De forma añadida, los atributos no relativos a la identidad también necesitan ser aprovisionados (por ejemplo, desde un servicio de directorio u otra fuente de atributos). Ambos tienen que ser aprovisionados a los PDPs/PEPs, y la puntualidad y la corrección juegan un papel crítico.

10.3.5.5 Gestión de políticas de acceso en Cloud

Hacer gestionable la creación y mantenimiento de políticas constituye un gran reto; casi siempre hay demasiadas reglas técnicas que gestionar, atributos y lenguajes de políticas usados que no son comprensibles para los administradores, reglas técnicas que necesitan ser actualizadas con frecuencia para que sigan siendo correctas después de cada cambio de sistemas (por ejemplo, en *mash-ups* de *Cloud* ágiles), y es difícil establecer el nivel de confianza/garantía en el que el nivel de aplicación de la política técnica se ajusta a las intenciones del administrador. Debido a todo esto, el planificar cuidadosamente las herramientas y procesos para poder hacer este proceso de creación y actualización de políticas de acceso a través de la automatización es crítico.

Las soluciones actuales incluyen aproximaciones automatizadas que convierten políticas de seguridad de alto nivel en reglas técnicas de acceso de bajo nivel, incluyendo:

- Seguridad dirigida por modelos⁸⁰, que se define como el proceso de modelar los requisitos de seguridad con un alto nivel de abstracción apoyándose en herramientas y usando otras fuentes de información acerca del sistema (producidas por otras partes interesadas). Estas entradas, que se especifican en DSL (*Domain Specific Languages* o Lenguajes de Dominio Específico) se transforman en reglas de seguridad aplicables con tan poca intervención humana como sea posible. También se incluye la gestión de la seguridad en tiempo de ejecución (por ejemplo, concesiones de autorización/autorizaciones), la aplicación en tiempo de ejecución de las políticas en los sistemas TIC protegidos, las actualizaciones de las políticas dinámicas y la monitorización de violaciones de las políticas.
- Agrupar las reglas de acceso técnicas en grupos similares para reducir la complejidad.
- Tratar de hacer las políticas técnicas más fáciles de entender a través de visualizaciones.

10.3.5.6 Mejores prácticas para la autorización en Cloud

- Considerar cuidadosamente si una perspectiva centrada en la protección de recursos para la creación de políticas de acceso es más adecuada al entorno que una centrada en las identidades.
- Garantizar la gestionabilidad de las políticas de acceso, especialmente en *mash-ups Cloud* que cambian dinámicamente. Esto incluye la consistencia de la creación de políticas, distribución de políticas, aplicación y actualización. Considerar el uso de herramientas y aproximaciones automatizadas (por ejemplo, seguridad dirigida por modelos) para generar las reglas de acceso técnicas necesarias para la aplicación de la política.
- Designar responsabilidades claras para la gestión y auditoría de políticas.

⁸⁰ NIST IR 7628

- Asegurarse de que el CSP ofrece PEPs/PDPs con gestión de la autorización que puedan ser configurados con la política de autorización específica del cliente, y que el servidor de políticas de la empresa puede interactuar correctamente con la política elegida.
- Considerar el uso de “política como servicio” para el servidor de políticas si es necesario un servidor de políticas central para un *mash-up Cloud*.

Mejores prácticas actuales para la selección de servicios de autorización:

- La característica más importante de un servicio de gestión de la autorización es la capacidad de gestión de la política del cliente *Cloud*, porque la gestión de las políticas de acceso es el problema más grande de la autorización.
- Los servicios deberían permitir la generación (¡y actualización!) de políticas técnicas desde requerimientos de política de seguridad genéricos e intuitivos de la forma más automatizada posible.
- Si es políticamente viable para la organización, y si es posible, debería considerarse como una opción de externalización la “política como servicio” para la creación y actualización de políticas. Esta opción es más aceptable entre *Cloud* comunitarias, donde la “política como servicio” se ofrece a una comunidad cerrada.
- Asegurar que los servicios tienen una función de exportación/importación de/desde estándares como XACML de OASIS.
- Comprobar que los servicios pueden interactuar con los PDPs/PEPs instalados en la infraestructura *Cloud* y con los puntos de monitorización de la política para las tareas de monitorización de incidentes y auditoría.

10.4 Test de intrusión de aplicaciones *Cloud*

Un test de intrusión consiste en evaluar las vulnerabilidades residuales presentes en la aplicación o capa de sistema que puedan ser potencialmente explotadas por un intruso externo o interno con intenciones maliciosas. El test supone habitualmente un análisis activo de las superficies de una aplicación o sistema como una “caja negra”, intentando identificar vulnerabilidades típicas frecuentes a causa de mala programación o un bastionado deficiente.

OWASP⁸¹ en su “Guía de Test OWASP V3.0” recomienda nueve categorías de test activos de seguridad:

1. Test de gestión de la configuración.
2. Test de lógica de negocio.
3. Tests de autenticación.
4. Tests de autorización.
5. Test de gestión de sesiones.
6. Test de validación de datos.

⁸¹ OWASP - Open Web Application Security Project, / Proyecto Abierto de Seguridad en Aplicaciones Web www.owasp.org

7. Test de denegación de servicio.
8. Tests de servicios web.
9. Test de Ajax (Test de seguridad RIA).

Las categorías de test de seguridad citadas arriba son igualmente aplicables para una aplicación que va a ser desplegada en *Cloud* ya que la naturaleza de las vulnerabilidades de aplicación no va a cambiar desde un punto de vista técnico. Sin embargo, dependiendo del tipo de modelo de despliegue *Cloud* se pueden tener vectores de amenaza adicionales (que podrían no entrar en la ecuación en un despliegue no *Cloud*).

Un ejemplo de dicho vector de amenaza en un despliegue SaaS podría ser provocado por la multipropiedad cuando el mismo entorno de ejecución de aplicación es usado para servir a varios clientes y sus datos segregados.

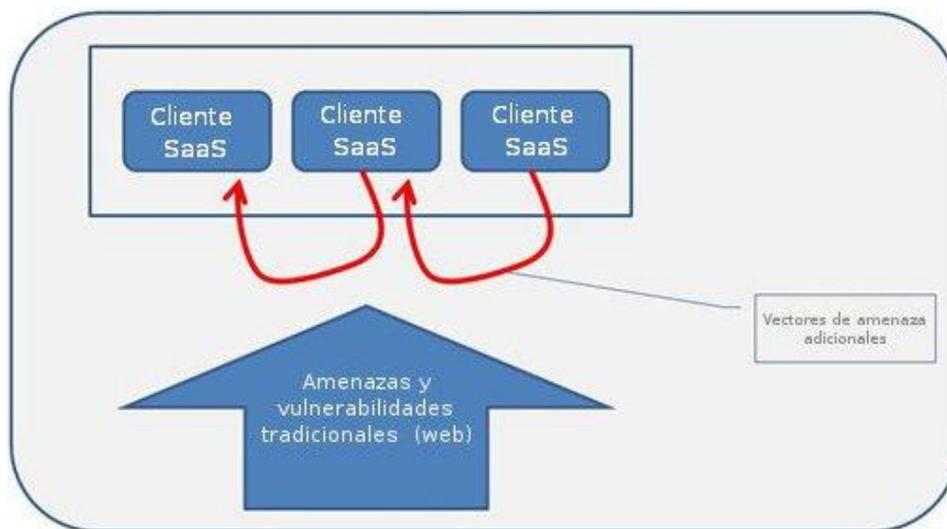


Figura 13— Herencia de vectores de amenaza

Será necesario desarrollar e incluir tipos adicionales de tests para tratar las amenazas que surjan como resultado de modelo de despliegue de la aplicación en *Cloud*. Un ejemplo de los mismos puede verse en la tabla siguiente

Tabla 8— Herencia de vectores de amenaza

MODELO DE CLOUD EN EL QUE SE DESPLIEGA LA APLICACIÓN	CAUSANTES DE AMENAZAS ADICIONALES	EJEMPLOS DE AMENAZAS	CATEGORÍAS DE TESTS DE SEGURIDAD TRADICIONALES QUE SON RELEVANTES	CATEGORÍAS ADICIONALES DE TEST
SAAS	Multi-tenancy a nivel de aplicación	Un cliente que usa la misma infraestructura SaaS logra acceder a datos de otros	<ul style="list-style-type: none"> ▪ Gestión de la Configuration ▪ Lógica de negocio ▪ Autenticación 	<ul style="list-style-type: none"> ▪ Test de multipropiedad (una extensión de la escalada de privilegios)

MODELO DE CLOUD EN EL QUE SE DESPLIEGA LA APLICACIÓN	CAUSANTES DE AMENAZAS ADICIONALES	EJEMPLOS DE AMENAZAS	CATEGORÍAS DE TESTS DE SEGURIDAD TRADICIONALES QUE SON RELEVANTES	CATEGORÍAS ADICIONALES DE TEST
		clientes a través de vulnerabilidades en la capa web (una escalada de privilegios)	<ul style="list-style-type: none"> ▪ Autorización ▪ Gestión de sesiones ▪ Validación de datos ▪ Denegación de servicio ▪ Servicios web ▪ Ajax (Test de seguridad de RIA) 	
PAAS	Multi-tenancy a nivel de plataforma	Idem?	Idem?	Idem?
IAAS	Multi-tenancy a nivel de infraestructura	Fallos en la seguridad de la virtualización (implementación defectuosa de las zonas de VM o de la segregación que conduce a ataques entre las VM de distintos clientes IaaS)	<ul style="list-style-type: none"> ▪ Evaluación de las vulnerabilidades tradicionales de la infraestructura (es necesario definir esto) 	<ul style="list-style-type: none"> ▪ Test de vulnerabilidades de seguridad entre VM

10.5 Monitorización de aplicaciones en *Cloud*

Como otros aspectos de la seguridad *Cloud*, qué y cómo se monitoriza un sistema basado en *Cloud* varía en función del tipo de *Cloud* bajo estudio. Qué significa monitorizar aplicaciones *Cloud* y cómo monitorizar diferentes tipos de aplicaciones *Cloud* se explica en detalle a continuación.

10.5.1 Monitorización de aplicaciones Cloud: Toma y daca

En este documento se limita el término “monitorización” a la monitorización de la seguridad de aplicaciones. En particular se deberían tener en cuenta las siguientes categorías de métricas:

- 1. Monitorización de logs:** No consiste en simplemente archivar los *logs* por motivos de cumplimiento legal. Hay que entender el potencial de la salida que se envía a esos *logs* y monitorizarlos en busca de posibles eventos. El *logging* de errores de una aplicación es inútil a menos que exista un proceso que detecte y responda a estos errores.
- 2. Monitorización del rendimiento:** Esta categoría juega un papel importancia en la computación compartida. Un cambio significativo en el rendimiento de una aplicación puede ser el síntoma de que otro cliente está usando una parte mayor de la que le corresponde de un recurso limitado (Ej. CPU, memoria, almacenamiento SAN), o puede ser síntoma de actividad maliciosa ya sea en la aplicación monitorizada o en cualquier otra aplicación dentro de la infraestructura compartida.
- 3. Monitorización de uso malicioso:** Esta categoría requiere una mezcla de auditoria y monitorización para ser exitosa. La empresa debe comprender lo que sucede cuando un usuario malicioso intenta conseguir acceso privilegiado, o emplear permisos que no posee. Los logs de auditoría deben de registrar los intentos de inicio de sesión fallidos (y los exitosos). ¿Guardan todo las funciones de validación de datos? Si una aplicación experimenta un aumento significativo de carga de tráfico, ¿se genera una alerta en algún lugar?
- 4. Monitorización de intrusiones:** En esta categoría la clave es la rapidez y eficiencia con la que una organización responde a la intrusión. Dependiendo de la complejidad de la aplicación, determinar que ha sido comprometida puede ser relativamente sencillo (por ejemplo, “el usuario A ha iniciado sesión dos veces”) o puede requerir más esfuerzo (por ejemplo, desarrollando algoritmos heurísticos que monitoricen el uso de datos). Esta categoría es un buen ejemplo de un elemento que, si se incluye de forma previa en el SDLC, puede ser más sencillo de gestionar.
- 5. Monitorización de la violación de políticas** (especialmente el control de accesos): Es importante también monitorizar cómo un PDP llegó a una decisión, es decir, qué reglas de la política se aplicaron para tomar una decisión de acceso específica. Esto se debe alinear con una aproximación a la monitorización dirigida por políticas que evite los típicos problemas de la monitorización (falsos positivos y sobrecarga de incidentes).

Estos son algunos conceptos clave detrás de la monitorización de *logs* – el “toma” de la ecuación. La misma importancia tiene el lado “daca”, del que es responsable el desarrollador de la aplicación: La aplicación debe proporcionar un sólido subsistema de *logging* para permitir que el sistema de monitorización haga su trabajo eficientemente:

- 1. Fácilmente analizable:** Se deberían escribir los *logs* en un formato que pueda ser analizado con facilidad por un sistema diferente. Una buena opción sería usar un formato ya aceptado y conocido como XML. Un mal ejemplo sería escribir los *logs* en formato de texto multilínea y sin definir.
- 2. Fácilmente legible:** A menos que se escriban los *logs* en un formato binario (que sin duda alguna nunca va a ser leído directamente por una persona), una entrada de *log* debería ser comprensible por una persona con un perfil técnico que esté familiarizada con la aplicación.
- 3. Bien documentada:** Escribir los *logs* en un fichero no es suficiente. Los códigos de error tienen que estar documentados y deberían de ser únicos. Si una entrada de *log* particular tiene una solución conocida, se debe documentar la solución o proporcionar una referencia a la misma.

10.5.2 Monitorizar aplicaciones en diferentes tipos de Cloud

En una aplicación basada en IaaS la monitorización es casi “normal”, similar a la de aplicaciones “legacy” desplegadas en entornos no compartidos. El cliente necesita monitorizar problemas con la infraestructura compartida o con intentos de acceso no autorizados a una aplicación por un co-propietario malicioso.

Monitorizar aplicaciones desplegadas en una *Cloud* PaaS requiere de trabajo adicional. A menos que el proveedor de la plataforma proporcione a su vez una solución de monitorización capaz de monitorizar la aplicación desplegada, el cliente tiene dos opciones: O escribe una lógica de aplicación adicional para realizar las tareas de monitorización dentro de la aplicación, o envía los *logs* a un sistema remoto de monitorización, ya sea el propio del cliente o un servicio ofrecido por una tercera parte.

Dado que las aplicaciones basadas en SaaS son las que ofrecen menor flexibilidad, no debería de ser una sorpresa que la monitorización de la seguridad de estos tipos de aplicaciones sea la más complicada. Antes de emplear un producto SaaS, los clientes deberían tener una comprensión completa de:

- ¿Cómo monitoriza el proveedor sus aplicaciones?
- ¿Qué tipo de información de auditoría, *log*, o información envía el proveedor al cliente? ¿Tiene el cliente la posibilidad de elegir qué información recibir?
- ¿Cómo transmite el proveedor esta información al cliente? (¿Twitter? ¿Email? ¿API personalizada?)

Por último, cuando se considera la monitorización de la seguridad de aplicaciones en el *Cloud*, es necesario tener en cuenta que mientras que los proveedores (o los servicios de monitorización *Cloud* de una tercera parte) pueden haber construido un sistema de monitorización para monitorizar las aplicaciones de un cliente, estos sistemas están monitorizando cientos, sino miles, de clientes. El proveedor, como negocio, quiere que su sistema de monitorización funcione “suficientemente bien”. Si el cliente posee los recursos, tener su propio sistema para monitorizar únicamente sus aplicaciones será casi siempre mucho más informativo y con mejor respuesta que el de un proveedor *Cloud*.

10.6 Recomendaciones

10.6.1 Recomendaciones para la garantía de la seguridad

- Se deben definir los requisitos funcionales, regulatorios y de privacidad que cumplan las necesidades del desarrollo y despliegue *Cloud*.
- Se debe realizar una evaluación detallada y los riesgos y vectores de ataque del entorno *Cloud*, y se deben integrar las estrategias de mitigación dentro de los requisitos.
- Se debe llevar a cabo una evaluación de impacto de los riesgos y vectores de ataque, y se deben documentar junto con las pérdidas o daños potenciales de cada escenario.
- Los requisitos y esfuerzos de seguridad y privacidad deberían de ser priorizados por posibilidad e impacto.

10.6.2 Recomendaciones para el análisis de riesgos

- Se deben realizar análisis de riesgos de las aplicaciones en lo relativo a la privacidad y la seguridad (confidencialidad, integridad y disponibilidad), y se deben construir y mantener modelos de amenazas.
- Se debe analizar el riesgo desde la perspectiva del desarrollo y el despliegue en *Cloud*, y se deben mantener modelos de las amenazas relacionadas.
- Se deben crear y mantener un catálogo de los vectores de ataque y el análisis de impacto específicos para arquitecturas *Cloud*.
- Se debe mantener la trazabilidad entre las capacidades de garantía de la seguridad y todas las amenazas y riesgos identificados.

10.6.3 Recomendaciones para la arquitectura

- Se deberían desarrollar y mantener marcos de referencia de arquitectura de software seguro.
- Se deberían usar patrones de arquitecturas de *Cloud computing* que reduzcan explícitamente las amenazas (por ejemplo, “Open Security Architecture”⁸² o TOGAF/SABSA).
- La arquitectura de la aplicación debe de tener bloques de construcción reusables que mitiguen los escenarios de fallos de seguridad más comunes.
- Se deben usar arquitecturas de datos seguras específicas para el *Cloud* que potencien el marco de referencia de arquitectura de seguridad, que tengan en cuenta aspectos y amenazas específicos como:
 - La monitorización de servidores de bases de datos dinámicas.
 - Comprensión de dónde está exactamente alojada la base de datos en cualquier momento.
 - Realizar un *logging* centralizado de toda la actividad entre distintos sistemas (potencialmente a nivel global) para proporcionar una visión holística de la aplicación y poder señalar eventos sospechosos.
 - Definir dónde se debe usar el cifrado (ver el Dominio 12).
 - Proporcionar una separación de tareas adecuada dentro del sistema, los datos y todas las actividades de privilegios de terceras partes, capaz de ser monitorizada por el personal de la organización dueña de los datos.

10.6.3 Recomendaciones para el test de intrusión en aplicaciones *Cloud*

- Realizar tests de intrusión de aplicaciones web con regularidad, revisando el Top10 de vulnerabilidades de OWASP.

⁸² www.opensecurityarchitecture.org

- Categorizar las vulnerabilidades basándose en su criticidad e impacto, y tener un proceso para remediarlas.
- Realizar test manuales desde una perspectiva de multipropiedad para validar que no se pueden escalar privilegios o acceder a datos por una falta de cumplimiento de las sesiones de la aplicación.
- Para aplicaciones que se vayan a migrar a un entorno IaaS o PaaS, es necesario realizar una evaluación de seguridad para garantizar que los controles de seguridad subyacentes como la segregación de VM y división en zonas, la seguridad de la virtualización, etc. han sido implantados correctamente y no ponen en riesgo al ecosistema de aplicaciones.

Referencias

- [1] The Building Security In Maturity Model. <http://bsimm.com/>
- [2] OpenSAMM – Software Assurance Maturity Model. <http://www.opensamm.org/>
- [3] DAVIS, NOOPUR. Secure Software Development Life Cycle Processes. Software Engineering Institute
- [4] SP-011: *Cloud Computing* Pattern. <http://www.opensecurityarchitecture.org/cms/en/library/patternlandscape/251-pattern-cloud-computing>
- [5] KRUTZ, RONALD L. and VINES, RUSSEL DEAN. 2010. *Cloud Security- A Comprehensive Guide to Secure Cloud Computing*. Wiley Publishing, Inc., Indianapolis, IN.
- [6] SARNA, DAVID E.Y. 2010. *Implementing and Developing Cloud Computing Applications*. Auerbach Publications.
- [7] BELK, MARK, COLES, MATT, et al. 2011. *Fundamental Practices for Secure Software Development: A Guide to the Most Effective Secure Development Practices in Use Today, 2nd EDITION*. Software Assurance Forum for Excellence in Code. http://www.safecode.org/publications/SAFECode_Dev_Practices0211.pdf
- [8] RITTINGHOUSE, JOHN W. and RANSOME, JAMES F. 2009. “*Cloud Security Challenges*” in *Cloud Computing: Implementation, Management, and Security*. Auerbach Publications.
http://www.infosectoday.com/Articles/Cloud_Security_Challenges.htm
- [9] *Guidelines on Security and Privacy in Public Cloud Computing*. Computer Security Division Information Technology Laboratory. 2011. National Institute of Standards and Technology - Gaithersburg, MD 20899-8930
http://csrc.nist.gov/publications/drafts/800-144/Draft-SP-800-144_cloud-computing.pdf
- [10] Homomorphic Encryption. Making *Cloud Computing* More Secure.
<http://www.technologyreview.in/computing/37197/>
- [11] *Cloud Data Protection. Best Practices*. <http://www.ciphercloud.com/blog/?cat=10>

DOMINIO 11 //

CIFRADO Y GESTIÓN DE CLAVES

Para un profesional de la seguridad, resulta obvio que si una organización necesita almacenar información y no confía en aquellos que pueden acceder o utilizar la misma, debe proceder a cifrarla. Por otro lado, cuando una organización dispone de *CPD* en el cual controla todos sus activos, la información se cifra, puesto que ciertas regulaciones exigen que los datos estén cifrados (i.e. *PCI DSS*).

En *Cloud*, donde hay muchos usuarios y administradores trabajando para terceros, parece obvio que será necesario cifrar mucha más información. En ese caso, ¿cómo funcionan esos procesos y cómo gestionan las organizaciones sus claves? Cifrar toda la información incrementa la complejidad. Por otra parte, ¿es verdaderamente necesario cifrar todo este volumen de información si, entre otras cuestiones, incrementa la complejidad de los procesos? ¿Existe otra manera de reducir la necesidad de cifrar información y consecuentemente reducir los procesos de gestión de claves? Este capítulo analiza estas cuestiones.

Introducción. Este dominio tratará los siguientes temas:

- Introducción al Cifrado
- Enfoques alternativos al Cifrado
- Criptografía en despliegues *Cloud*
- Cifrado en bases de datos *Cloud*
- Gestión de claves en *Cloud*
- Almacenamiento y custodia de claves

***¿Cifrar o no cifrar? Esa es la cuestión.
En caso afirmativo, ¿cómo gestiono
las claves? Si no, ¿son los riesgos
demasiado altos?***

11.1 Introducción al Cifrado

La información clasificada como confidencial, tanto debido a requerimientos regulatorios como de secreto corporativo, debe ser protegida. Puesto que la información confidencial, que actualmente se gestiona mediante los sistemas internos, se migra cada vez más a *Cloud*, debe ser protegida con la misma diligencia. Sin embargo, migrar información a *Cloud* no elimina ningún requerimiento de confidencialidad y de protección de datos. Por tanto, la pérdida de control sobre la información fuera del perímetro corporativo (*de-perimetrization*) incrementa la complejidad de la protección de la información así como el riesgo de que ésta se vea comprometida.

Existen un conjunto de factores a considerar en relación al cifrado de la información en *Cloud*, incluyendo:

- Para proteger la información mediante cifrado, no es suficiente con el uso de un canal de transferencia de datos seguro (i.e. TLS), dado que el cifrado en la transmisión de información a *Cloud* no garantiza que la información esté protegida en *Cloud*. Una vez que la información llegue a *Cloud*, debería permanecer protegida tanto cuando esté siendo utilizada como cuando no.
- Para los ficheros no estructurados que necesiten ser protegidos tanto cuando estén almacenados como cuando estén siendo compartidos en *Cloud* aplicar siempre y cuando se pueda, la protección directamente a los ficheros, un cifrado embebido en el formato del fichero.

- Entender como las claves de cifrado serán gestionadas a lo largo del ciclo de vida de la información. Siempre que sea posible, evitar confiar en un proveedor de *Cloud* para proteger y utilizar apropiadamente las claves que protegen tu información crítica.
- Evitar que se puedan producir excepciones en el cumplimiento de las medidas preventivas de seguridad por empleados de terceras partes, así como legislaciones regionales que puedan requerir accesos indeseados, pero obligatorios, a tus ficheros cifrados. Si sólo tú dispones de las claves, sólo tú puedes acceder a tus ficheros.
- No olvidar proteger aquellos ficheros que habitualmente se pasan por alto, pero que frecuentemente contienen información sensible. Por ejemplo, ficheros de log y metadatos pueden ser vías a través de las cuales se originen pérdidas de datos.
- Utilizar técnicas de cifrado fuertes (como AES-256) que cumplan con los mismos requerimientos corporativos y regulatorios aplicados a los ficheros mantenidos internamente. Utilizar formatos abiertos y validados, evitando en la medida de lo posible, el uso de técnicas de cifrado propietario.

11.2 Enfoques alternativos al Cifrado

Existen muchos motivos para valorar enfoques alternativos al cifrado de la información en *Cloud*. Para muchas organizaciones, el envío de información a *Cloud* es equivalente a transferir su custodia.

Las alternativas para aquellas organizaciones que tengan dudas a la hora de enviar información no segura fuera de la organización pueden ser:

- **Uso de tokens:** Integrar / paralelizar un servicio de *Cloud* público con un servicio de *Cloud* privado que almacene información sensible. La información enviada a *Cloud* público se altera, conteniendo solamente una referencia a la información almacenada en *Cloud* privado.
- **Disociación de la información.** Alteración de (por ejemplo) información personal (**PII**) e información sensible (**SPI**)⁸³ antes de ser procesada.
- **Utilización de los controles de una base de datos *Cloud*.** Empleo de los controles de acceso implementados sobre la base de datos, de forma que provean niveles adecuados de segregación.

Como regla general, las buenas prácticas en la gestión de datos son esenciales antes de migrar la información a *Cloud*, con el objeto de diferenciar si toda la información necesita ser cifrada o sólo parte, si necesita ser protegida mediante un método alternativo, o si no necesita ser protegida.

Los riesgos derivados de la compartición de información, que deben ser considerados al evaluar qué información proteger y mediante qué métodos, pueden ser divididos en dos categorías principales: divulgación o uso indebido, y catalogados en las siguientes áreas:

- **Divulgación pública accidental.** Habilitar el acceso del público general a la información a través de una publicación o post en la web.

⁸³ SPI - Sensitive Personal Information

- **Divulgación accidental o maliciosa.** El acto de facilitar la información a uno o varios terceros como resultado de una protección inadecuada.
- **Divulgación forzada a terceros.** La obligación de revelar determinada información por requerimiento judicial.
- **Divulgación a entidades gubernamentales.** La divulgación de la información a entidades gubernamentales, por motivos legislativos u orden judicial (por ejemplo, el *Patriot Act* en EEUU).
- **Uso indebido de perfiles de usuario o de red.** La habilidad de, partiendo de tráfico de datos aparentemente benigno, analizar y revelar comportamientos, asociaciones, preferencias o intereses de un usuario, mediante minería de datos.
- **Uso indebido de la inferencia.** Ser capaz de sintetizar identificadores de primer o segundo orden para deducir la identidad o el comportamiento de una persona.
- **Re-identificación y reversión de la disociación de datos.** Disponer de suficiente información anónima como para deducir el sujeto original.

11.3 Cifrado en Despliegues Cloud

Hay dos conceptos complementarios que se utilizan en temas de cifrado:

- **Content Aware Encryption** (Cifrado en función del contenido). Utilizado para la prevención de pérdidas de información (*Data Leak Prevention*), cifra las diferentes tipologías de datos o formatos en base a los parámetros definidos en una política. Por ejemplo, el cifrado de un número de tarjeta de crédito cuando se envía un correo electrónico a las autoridades pertinentes.
- **Format Preserving Encryption** (Cifrado con conservación de formato). Cifrado de un mensaje con un resultado es similar al mensaje de entrada. Por ejemplo, un número de tarjeta de crédito de 16 dígitos sigue siendo un número de 16 dígitos tras el cifrado; un número de teléfono parecerá un número de teléfono y una palabra en español, parecerá una palabra en español.

La forma preferida de proteger la información es enviarla cifrada desde las organizaciones a *Cloud* sin la intervención del usuario. El cifrado en función del contenido puede ser potenciado en *Clouds* públicas, siempre y cuando el software pueda ser configurado para cifrar también en función del protocolo, permitiendo cifrar campos en una transacción REST http a una aplicación de una *Cloud* pública. Las pérdidas de información (**DLP**)⁸⁴ pueden ser prevenidas con productos que refuerzan la protección de los datos que salen de la compañía, normalmente por correo electrónico, cifrando la información antes de su salida. Este principio puede ser utilizado en la protección de la información en *Cloud*. Sin embargo, el producto *DLP* permite generar alertas, mientras que un servicio de seguridad en función del contenido debería detectar, cifrar y trazar, pero no emitir alertas.

El cifrado de conservación de formato va un paso más allá que el cifrado en función del contenido, puesto que identifica la información que necesita ser cifrada y mantiene el formato y el tipo de dato. Por ejemplo, el empleo del cifrado

⁸⁴ **Data Leak Prevention (DLP)** o pérdida de información: Los productos DLP detectan información que sale de un dispositivo seguro o de la organización, cifrándola.

convencional en una tarjeta de crédito haría que el texto cifrado (**cipher-text**⁸⁵) ya no fuera un número de 16 dígitos. El cifrado de conservación de formato generaría un texto de 16 dígitos, además de cifrarlo.

Preservando el tipo de dato y el formato, el sistema de cifrado puede cambiar fácilmente valores, de acuerdo a una amplia gama de protocolos. El reto clave del cifrado de conservación de formato es la encriptación de grandes volúmenes de texto en plano, como un correo electrónico almacenado en *Cloud*. La encriptación masiva se realiza normalmente utilizando cifrado en bloque (**ciphers**⁸⁶). El cifrado de conservación de formato permite que el cifrado sea un conjunto de caracteres de la misma longitud que el texto original, por lo que texto cifrado puede ser almacenado en campos del mismo tipo que el texto plano original, pero con el inconveniente del tiempo.

El cifrado en aplicaciones *Cloud* plantea ciertos problemas para las aplicaciones del negocio que deben ser abordados por la arquitectura de las mismas:

- Si el dato se requiere para la búsqueda de registros u objetos en la aplicación, entonces el uso de una clave primaria⁸⁷ cifrada dificultaría el proceso.
- La gestión de claves se complicará en caso de que el conjunto de aplicaciones *Cloud* contenga procesos *batch* u otro tipo de procesos que traten información sensible, particularmente PII y SPI, y dichos procesos sean migrados a *Cloud*.

Una aplicación que necesita encontrar registros u objetos en una base de datos, puede preferir emplear otro modo para almacenar un valor único, como el uso de *tokens*. Los *tokens* son utilizados habitualmente en el entorno de las tarjetas de crédito para asegurar que el número de tarjeta es accedido lo mínimo posible por las aplicaciones. Un único *token* generado de un valor puede ser utilizado para desarrollar una nueva clave primaria, que la aplicación puede utilizar sin exponer datos sensibles en un *Cloud* público.

Tal y como se explicará en la sección 11.4, preferentemente, las claves no deberían ser almacenadas en *Cloud* sino que deberían ser mantenidas por la organización cliente o por un proveedor de gestión de claves de confianza.

Los procesos que necesitan trabajar sobre información sin cifrar y ser ejecutados en *Cloud* con otras aplicaciones e información del negocio, deben tener acceso a las claves o al servicio de gestión de claves para llevar a cabo sus funciones. Consultar la sección 11.4 para más detalles en relación a la gestión de claves en *Cloud*.

11.3.1 Cifrado en bases de datos *Cloud*

Lo primero a considerar es si es necesario cifrar la información. Todas las bases de datos permiten restringir el acceso a la información, lo cual implementado adecuadamente, puede ser suficiente para proteger la confidencialidad.

Otras razones que pueden requerir el uso de cifrado para proteger la información almacenada en la base de datos son:

- Ocultar la información de aquellos usuarios con acceso privilegiado a la base de datos (administradores de bases de datos (**DBAs**)⁸⁸, por ejemplo).

⁸⁵ **Cipher text** - El resultado de una operación de cifrado. La entrada se denomina texto en claro.

⁸⁶ **Ciphers** - Software / Hardware basado en un algoritmo que realiza cifrado/descifrado y firma/verificación.

⁸⁷ **Clave primaria** - Columna/campo/atributo de una base de datos que se utiliza para identificar unívocamente los registros de la base de datos.

- Cumplir con requerimientos legales (como la ley *SB1386* de California).
- Almacenar la información en un esquema en el cual el dueño de la información no pueda controlar las credenciales de la cuenta accediendo a la información (utilizando cuentas compartidas, por ejemplo).

Al utilizar una base de datos *Cloud* y particularmente una solución *SaaS* que emplee una base de datos, la capacidad de la base de datos de funcionar correctamente puede verse comprometida si no dispone de acceso a las claves, salvo que pueda operar con información cifrada.

El cifrado de información incrementa la complejidad y reduce el rendimiento, aunque, existen alternativas efectivas:

- **Utilización de la Seguridad a nivel de objetos.** Uso de las instrucciones SQL *grant* (conceder) y *revoke* (revocar) para restringir qué cuentas pueden acceder a la información. Las cuentas a las que se les conceda acceso deben estar controladas, para asegurar que el acceso está siendo concedido solamente a usuarios autorizados.
- **Almacenamiento de un hash seguro.** En vez de almacenar la información directamente, almacenar un *hash*. Esto permite que el programa verifique que el titular dispone del valor original ni necesidad de almacenarlo.

11.4 Gestión de claves

Uno de los procesos más complejos del *Cloud computing* público es la gestión de claves. Los modelos multi-usuario de las soluciones *Cloud* públicas, originan problemas de gestión de claves para aquellos procesos que se ejecutan en *Cloud*.

Los casos más sencillos son aquellos en los que existen aplicaciones ejecutándose en *Cloud* público, y en los que las claves que cifran la información enviada a *Cloud* desde las organizaciones son sólo utilizadas en las propias organizaciones. Tal y como se describe en la sección uno, existen mecanismos de cifrado que permiten cifrar la información durante su envío a *Cloud* y descifrarlo a su regreso. Una aplicación que utilice claves criptográficas puede ver complicada su ejecución cuando otros procesos, tales como procesos *batch*, se ejecuten en *Cloud* y necesiten acceso a las claves para descifrar información.

Los usuarios del cifrado en las organizaciones necesitan disponer de claves propias de tal manera que no se utilice una única clave a lo largo de la organización. La manera más fácil de cumplirlo es mediante la utilización de un mecanismo de cifrado para cada usuario o entidad, lo que permite disponer de claves asignadas (y gestionadas) en base a la identidad de las entidades. De esta forma, cualquier cifrado que se realice específicamente para una entidad es gestionado para dicha entidad específica. Si una entidad necesita compartir en un grupo el acceso a la información, se pueden establecer claves a nivel de grupo, que pueden asociarse con la aplicación que gestiona el acceso de los grupos, y compartidas por las entidades pertenecientes a dicho grupo. Por otra parte, las claves deberían ser gestionadas en la organización tal y como ya se ha comentado en esta sección.

Si la información está almacenada en un entorno de *Cloud* público, pueden existir problemas a la hora de demostrar que toda la información (especialmente PII y SPI, u otros datos sujetos a marcos regulatorios) ha sido eliminada del entorno *Cloud*, incluyendo los dispositivos, tales como cintas de copias de seguridad. El disponer de una gestión local de claves permite garantizar que toda la información que no haya sido eliminada en el *Cloud* público no podrá ser descifrada tras revocar, borrar o perder, las claves del sistema de gestión de claves.

⁸⁸ DBA – Database Administrator (Administrador de base de datos)

11.4.1 Almacenamiento y custodia de claves

Sin embargo, el cifrado de información posee un valor limitado en caso de que ambos proveedores, así como los usuarios de los servicios de *Cloud*, no refuercen los procesos relativos a la gestión de claves.

Por parte del proveedor, una carencia de **SOD**⁸⁹ (Segregación de funciones) en relación al acceso a los servidores de claves, así como al acceso a los servidores con información cifrada debería ser un motivo de preocupación. Otras áreas de riesgos son el que los **DBAs** dispongan de acceso a las claves individuales de las bases de datos, o que la arquitectura del servicio de base de datos recaiga en una única clave.

Soluciones tales como el establecimiento de controles para proteger las claves, mediante el uso de **KEK**⁹⁰ (Clave de Cifrado de Claves), la generación de claves cifradas en memoria, y el almacenamiento únicamente de las claves cifradas de los servidores cifrados, son soluciones válidas que deben ser consideradas a la hora de diseñar cualquier solución.

Por otro lado, también deberían ser un motivo de preocupación las claves gestionadas por parte del cliente que protejan claves almacenadas en dispositivos no seguros (tales como dispositivos móviles) o dispositivos que no dispongan del mismo nivel de controles que el sistema de cifrado.

11.5 Recomendaciones

Recomendaciones Generales

- La utilización de mejores prácticas a la hora de gestionar claves en caso de usar cualquier tipo de producto de cifrado/descifrado.
- El uso de tecnología comercial de proveedores confiables, a fin de emplear las mejores prácticas.
- Utilizar las mejores prácticas en la gestión de claves obteniendo, de una fuente fiable, la tecnología y productos para realizar el cifrado, descifrado, firma y verificación.
- Es altamente recomendable que las organizaciones mantengan sus propias claves o que hagan uso de un servicio de cifrado de un proveedor confiable.
- Si una organización necesita ejecutar un análisis u otro proceso que requiera información almacenada en *Cloud*, la organización debería desarrollarlo sobre una plataforma, como *Hadoop*, y derivar la información necesaria desde *Cloud*. Tales plataformas, incluyendo *Hadoop*, disponen de su propio conjunto de excepciones de seguridad, pero éstas quedan fuera del alcance de este capítulo.
- El alcance de las claves puede ser gestionado a nivel de individuo o de grupo.
- El acceso a nivel de grupo puede ser gestionado con tecnologías avanzadas, tales como sistemas **DRM** (Gestión digital de derechos) y otro software que se ejecute en el escritorio o portátil y que cifren discos, carpetas y mensajes de correo.

⁸⁹ **SOD** Segregation of duties - Segregación de funciones

⁹⁰ **KEK** Key Encrypting Keys - Clave de Cifrado de Claves

Cifrado en bases de datos

- Utilizar algoritmos estándar. No inventar / utilizar técnicas propias de cifrado. Los algoritmos de cifrado propios no se encuentran adecuadamente probados y son superados fácilmente.
- Evitar utilizar estándares antiguos de encriptación tales como *Data Encryption Standard (DES)*⁹¹.
- Hacer uso de la seguridad de los objetos. Se debería utilizar la seguridad básica a nivel de objetos (comandos *grant* y *revoke* de SQL) para prevenir el acceso a, incluso, la información cifrada.
- No cifrar claves primarias o columnas indexadas. Si se cifra una clave primaria, se deberán cifrar todas las claves externas que la referencien. Si se cifra una columna indexada, puede ocasionar que la ejecución de las consultas sea lenta cuando traten de usar el valor cifrado.
- Utiliza un enfoque de cifrado por columnas, dado que es el utilizado en los grandes sistemas de datos.

11.6 Requerimientos

- ✓ Con el objetivo de mantener las buenas prácticas y cumplir los requerimientos de las auditorías, la organización debería gestionar sus propias claves, o ser llevado a cabo por proveedor confiable de servicios de cifrado.
- ✓ Las claves utilizadas en tecnologías de cifrado ya existentes, como **DRM** y productos de cifrado de discos, deberían ser gestionadas a través de tecnologías de almacenamiento centralizadas e internas en la compañía. Los **HSM** (Hardware Security Modules) deberían ser utilizados para almacenar las claves, así como las operaciones criptográficas de procesos tales como cifrado/descifrado, firma y verificación.
- ✓ Los usuarios de la organización deberían seguir un proceso de registro para disponer de acceso a las operaciones de cifrado, por ejemplo mediante sistemas de Preservación de Formato (Formar *Preserving*) o Dependientes del Contenido (*Content Aware*), de forma pueden acceder a las claves de cifrado/descifrado en caso que sea necesario.
- ✓ Desplegar tecnología integrada con los sistemas corporativos que se base en la identidad de todos los componentes del ciclo del proceso para tomar decisiones acreditadas.
- ✓ Gestionar las claves utilizadas por los procesos criptográficos mediante el uso de operaciones criptográficas vinculantes.
- ✓ Utilizar sistemas existentes como **E-DRM**⁹² o **DLP** en caso de que sea posible.
- ✓ Las operaciones criptográficas vinculantes y la gestión de claves en los sistemas corporativos de gestión de identidades proporcionarán a la organización una integración más flexible, utilizando tecnologías que la organización sabe que funcionan y que han sido auditadas y revisadas.

⁹¹ **DES** - Data Encryption Standard

⁹² **E-DRM** - Enterprise Digital Rights Management. Proceso que protege contenido, como las comunicaciones corporativas internas o el material con copyright.

DOMINIO 12 //

IDENTIDAD, ASIGNACIÓN DE DERECHOS, Y GESTIÓN DE ACCESOS

Los conceptos de identidad, asignación de derechos (*Entitlement*) y gestión de accesos utilizados en computación tradicional requieren cambios de enfoque fundamentales cuando se implementa un entorno *Cloud*, particularmente al dividirlo en tres funciones distintas, identidad, asignación de derechos y gestión de Autorizaciones/Accesos (IdEA - Identity, Asignación de derechos, and *Authorization/Access Management*).

Para la mayoría de las organizaciones, implantar una aplicación tradicional significa implica implantar un servidor, posiblemente en una **DMZ**⁹³, y en muchos casos sujeto a un Servicio de Directorio (**DS**)⁹⁴ (como *Microsoft Active Directory*, *Novell eDirectory* u *Open LDAP*) para la autenticación de usuarios. En algunos casos significa implementar una aplicación o usar un servicio basado en web utilizando su sistema de autenticación independiente.

En comparación, una identidad en un servicio *Cloud* o aplicación bien implantados serian consumidos desde una gran variedad de fuentes externas junto con los atributos asociados (recordemos que una identidad se aplica no solo a los **Usuarios**⁹⁵, si no también a los Dispositivos, **Código**⁹⁶, Organizaciones y Agentes todos los cuales tienen identidad y atributos). Hacer uso de todas las múltiples identidades y atributos implicados en una transacción permiten al sistema *Cloud* tomar mejores decisiones globales basadas en riesgos (definidas por el **proceso de asignación de derechos**⁹⁷ e implementadas por los componentes de la gestión de autorizaciones y accesos) sobre los accesos granulares al sistema, procesos y datos dentro del sistema/aplicación *Cloud*.

Este proceso de uso de múltiples fuentes de Identidad y sus atributos relacionados es crítica cuando una aplicación *Cloud* es probable que se publique en Internet, y es probablemente también uno de los mayores obstáculos para las organizaciones que quieren utilizar servicios *Cloud* “reales” y optan en cambio por implementar tecnologías de virtualización en su propia DMZ conectadas a su propio DS interno.

Este enfoque **des-perimetrizado**⁹⁸ a la Identidad, gestión de derechos, y gestión de acceso proporciona una aproximación más flexible y segura pero también puede ser implementado igualmente bien dentro de los límites corporativos (o perímetro).

Introducción. Las secciones siguientes cubren aspectos claves de Identidad, Gestión de derechos y Gestión de Acceso) en un entorno *Cloud*:

- Introducción a la Identidad en un entorno *Cloud*
- Arquitectura de la Identidad para *Cloud*

⁹³ **DMZ** - DeMilitarized Zone

⁹⁴ **DS** o "Directory Service" se usa en esta sección como abreviatura para cualquier servicio corporativo de directorio genérico, utilizado para códigos de usuario y contraseña de acceso.

⁹⁵ Típicamente personas; para una definición mas amplia referirse a:

www.opengroup.org/jericho/Jericho%20Forum%20Identity%20Commandments%20v1.0.pdf

⁹⁶ Incluye todas las formas de código, hasta aplicaciones y datos auto protegidos.

⁹⁷ "Entitlement" o "**asignación de derechos**" es el proceso de asignar privilegios (p.e., acceso a una aplicación o sus datos) a las identidades y sus atributos relacionados.

⁹⁸ **Des-perimetrizado** o "*De-perimeterization*" en un término acuñado por el *Jericho Forum*[®] (www.jerichoforum.org)

- Federación de Identidades
- Aprovisionamiento y gobierno de la Identidad y Atributos
- Gestión de la Autorización y Acceso
- Arquitecturas de interfaz con proveedores de Identidad y Atributos.
- Nivel de confianza con Identidades y Atributos
- Aprovisionamiento de cuentas en Sistemas *Cloud*
- Diseño de Aplicaciones para la Identidad
- Identidad y Protección de Datos

12.1 Terminología Utilizada en este Documento

El lenguaje utilizado en torno a la identidad es confuso, con algunos términos con significados diametralmente opuestos para distintas personas. Para evitar confusión al leer este dominio, se definen algunos de los términos utilizados:

- **Identidad.** Medios por los que una *Entidad* puede ser completa y consistentemente identificada como única.
- **Identificador.** Los medios por los que una *Identidad* puede verificarse criptográficamente, normalmente utilizando tecnologías de clave pública.
- **Entidad.** Las diferentes tipologías que tendrán *Identidad*; estos son Usuarios, Dispositivos, Código, Organizaciones y Agentes.
- **Asignación de Derechos (Entitlement).** El proceso de asignar derechos o privilegios (por ejemplo, acceso a una aplicación o sus datos) a las *Identidades* y los *Atributos* relacionados.
- **Login Reducido (RSO).** El uso de una cuenta y/o una herramienta de sincronización de credenciales para minimizar el número (normalmente nombre de usuario y contraseña) que un usuario tiene que recordar; la mayoría de estas soluciones conllevan un compromiso en la seguridad.
- **Single Sign On (SSO).** La capacidad de pasar *Identidad* y *Atributos* hacia un servicio *Cloud*, de forma segura, usando estándares seguros como **SAML** y **OAuth**.
- **Federación.** La conexión de un repositorio de *Identidad* con otro.
- **Persona.** *Identidad* y los *Atributos* particulares que proporcionan el contexto al entorno dentro del cual la Entidad está operando. Una *Persona* puede ser una agregación de una *Identidad* individual con una *Identidad* organizativa y *Atributos* organizativos (un ejemplo de una *Persona* corporativa, Juan Pérez como Presidente de Empresa S.A., o un PC perteneciente a Empresa S.A.).
- **Atributos.** Facetas de una *Identidad*

12.2 Introducción a la Identidad en un Entorno *Cloud*

Un ecosistema de identidad se enfrenta a problemas incrementales (conceptualmente como mudarse de un pequeño pueblo donde cada uno conoce a los demás a una gran ciudad). A medida que la industria expande los sistemas de identidad desde un ordenador individual a una empresa global de ella a modelos de despliegue *Cloud*, la capacidad de identificar todas las entidades implicadas en una transacción se vuelve significativamente más difícil.

Sin embargo, en *Cloud*, el uso de *Identidad* para todas las *Entidades* en la cadena de valor de la transacción, y el cambio a decisiones basadas en el riesgo, no solo mitigan este si no que potencialmente mejoran la seguridad.

Los siguientes puntos clave tienen que tenerse en cuenta al implementar una solución basada en *Cloud* que precise el uso de información de identidad:

- La solidez con la que una *Identidad* puede ser validada alimentará el cálculo de riesgo cuando se interactúe con tal *Identidad* (como ejemplo; anónima, auto-declarada, validada por una organización reputada con una fuerte validación de *Identidad* organizativa).
- Los *Atributos* de una *Persona*, como la *Identidad*, tendrán una solidez con la que un *Atributo* puede validarse que alimente el cálculo de riesgo cuando interactúe con esa *Persona*. El grado de solidez irá desde auto-declarada a alidada por una organización conocida reputada (con una fuerte validación de *Identidad* organizativa).
- Identidad y Atributos tendrán que ser consumidos desde múltiples fuentes, de esta manera las soluciones/arquitecturas *Cloud* tendrán la capacidad de consumir fuentes múltiples y dispares de Identidad y Atributos.
- Habrá casos en los que una Identidad transitoria es suficiente (información suficiente de una Entidad para estimarla única).
- Habrá casos en los que donde será deseable un semi-anonimato (como una votación).

12.3 Arquitectura de Identidad para *Cloud*

El traslado desde una arquitectura tradicional de una organización delimitada, con aplicaciones tradicionales basadas en servidor, en centros internos de datos proporciona poca flexibilidad a una organización. El traslado hacia arquitecturas basadas en *Cloud* permite una mayor flexibilidad, ya sea desplegada internamente dentro de los límites de la organización (*Cloud* privada) o *Cloud* pública externa (SaaS, PaaS o IaaS).

La tabla 9 muestra como la identidad variará entre la implementación tradicional y la implementación *Cloud*, dependiendo del tipo de arquitectura *Cloud* implementada.

Tabla 9—*Afirmaciones Arquitectura de la Identidad*

TIPO ARQUITECTURA	ARQUITECTURA TRADICIONAL	ARQUITECTURA CLOUD
Interna / Perimetrizada	Conectada al DS interno Las Identidades deben mantenerse dentro del DS para ser utilizadas por la aplicación, utilizando potencialmente soluciones RSO sign-on reducido.	Capacidad para aceptar múltiples fuentes de <i>Identidad</i> y <i>Atributos</i>

TIPO ARQUITECTURA	ARQUITECTURA TRADICIONAL	ARQUITECTURA CLOUD
Interna / Des-perimetrizada	Requiere un control firme y conexión con los servicios corporativos utilizando túneles VPN. Es una arquitectura no recomendada.	Utiliza declaraciones para proporcionar <i>Identidad y Atributos</i> para el acceso a los servicios <i>Cloud</i> .
Externa / Perimetrizada	El alojamiento externo implica la extensión del perímetro hasta el proveedor del servidor. La <i>Identidad</i> se extiende a un entorno que el cliente no gestiona, a menudo situando una réplica del DS en ese entorno por motivos de rendimiento.	Utiliza declaraciones para proporcionar <i>Identidad y Atributos</i> para el acceso a los servicios <i>Cloud</i> .

Mientras que en la arquitectura tradicional “IAM (GIA)”⁹⁹, a menudo todos los componentes son independientes como partes de un único servidor, una arquitectura *Cloud* es potencialmente mas compleja tomando la *Identidad y Atributos* de varias fuentes y tomando las decisiones de autorización/acceso mediante un conjunto de reglas de asignación de derechos (Entitlement) definidas por el correspondiente proceso de asignación de derechos.

En la Figura 14, *Identidad y Atributos* son originarios de (potencialmente) múltiples orígenes y alimentan una capa de

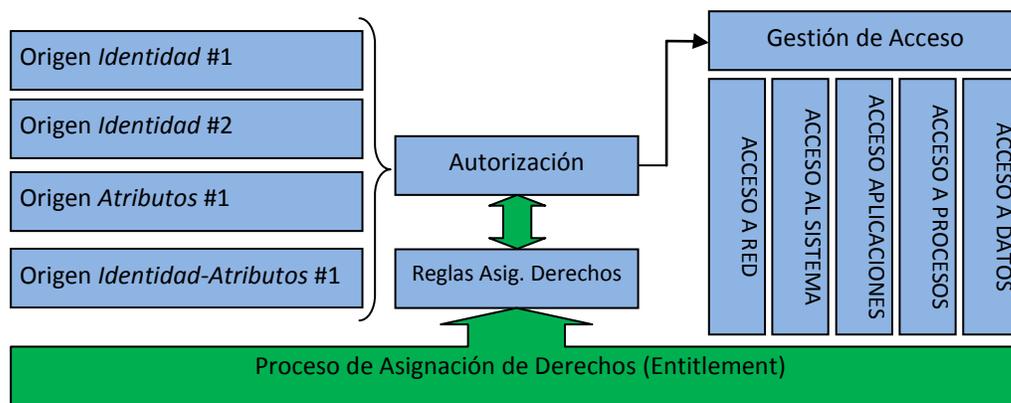


Figura 14: Sistema Genérico de Identidad, Asignación de Derechos y Gestión de Acceso

gestión de autorización/acceso que traduce las reglas de asignación de derechos en acceso.

La gestión de acceso deberá gobernar (dependiendo de los requisitos de negocio/seguridad, y el tipo de modelo *Cloud*, IaaS, PaaS o SaaS que se despliegue) el acceso a:

- **Capa de red.** Sin cumplir las reglas de asignación de derechos no sería incluso posible “ver” (por ejemplo usando ping o route) el sistema *Cloud*. Las reglas de asignación de derechos pueden también dirigir el acceso a interfaces concretas.

⁹⁹ IAM-Identity and Access Management, GIA-Gestión de Usuarios y Accesos

- **Capa de sistema.** Las reglas de asignación de derechos pueden definir los protocolos que se permiten para acceder y modificar sistemas, como por ejemplo servicios de terminal o web.
- **Capa de Aplicación:** Las reglas de asignación de derechos pueden mapear *Identidad* y/o *Atributos* a una funcionalidad proporcionada por una aplicación específica, como presentarla con un conjunto reducido de menús y opciones.
- **Capa de Proceso.** Las reglas de asignación de derechos pueden utilizarse para definir los procesos (o funciones) que pueden ser ejecutadas dentro de una aplicación. La asignación de derechos puede también definir que funciones mejoradas (como transferencias financieras fuera del ecosistema) necesitan verificación adicional (la cual puede obtenerse directamente o bien derivada en origen).
- **Capa de Datos.** Las reglas de asignación de derechos pueden limitar el acceso a áreas de los datos y la estructura de ficheros o incluso a ficheros individuales o campos dentro de los ficheros. (por ejemplo una base de datos). A un nivel mas avanzado, estas reglas podrían ser utilizadas para auto redactar documentos, como que dos usuarios accedan al mismo documento y vean distinto contenido (por ejemplo construyendo una vista dinámica de una tabla de base de datos)

El proceso de asignación de derechos comienza cuando el usuario convierte los requisitos de negocio y de seguridad en un conjunto de reglas de asignación de derechos. Este proceso definirá las *Identidades* y *Atributos* requeridos para ser capaz de evaluar las reglas. Estas reglas a su vez manejan el sistema de autorización/acceso.

12.4 Federación de Identidades

Conceptualmente hablando, la federación es la interconexión de Servicios de Directorio separados. Algunas organizaciones optan por un Gateway de federación, (un “Bridge” o “hub de Federación”) para externalizar su implementación de federación, donde la federación y las reglas por las que la Identidad se gestiona dentro del “bridge” se gobiernan por un conjunto de reglas, normalmente un contrato legal, permitiendo así acceso a otros socios de este “bridge” un nivel definido de confianza en identidades no emitidas directamente por ellos.

Tecnológicamente hablando, la federación es el uso de SAML para ofrecer portabilidad a dominios de seguridad independientes y separados de ciertas organizaciones que extienden su entorno DS a través de un producto Gateway que maneja declaraciones SAML. Otras organizaciones consumirán declaraciones nativas SAML de un servicio de identidad.

En ambos tipos de arquitecturas de federación, es esencial comprender la proveniencia de la *Identidad* y *Atributos* que están siendo declarados.

Los estándares de federación están siendo ampliamente utilizados en los modelos de despliegue SaaS tanto para federación de identidades como control de acceso. No existen estándares similares para modelos de despliegue PaaS o IaaS. Los clientes *Cloud* que hacen uso de modelos de despliegue IaaS deben tener en consideración como manejan el ciclo de vida de las identidades (cuentas compartidas, cuentas nominales, cuentas privilegiadas, etc.). Las empresas que hacen uso de herramientas PIM (Privileged Identity Management) para SUPM (Super User Management) y SAPM (Shared Account Password Management) deben investigar la extensión de estas herramientas para soportar despliegues *Cloud*. Tanto empresas y clientes *Cloud* deben tener bien definida una política de HPA (Highly Privileged Access).

12.5 Aprovisionamiento y Gobiernos de la Identidad y Atributos

En relación con el aprovisionamiento, típicamente se piensa en aprovisionamiento de usuarios, pero para tomar decisiones valiosas, basadas en el riesgo, los sistemas / aplicaciones *Cloud* necesitan *Identidad* y *Atributos* de todas las entidades implicadas en la transacción y potencialmente otros *Atributos* de otros sistemas / procesos.

Algunos ejemplos *Identidad* y *Atributos* son: (no es una lista exhaustiva):

- Declaración de Usuario: *Identificador de Usuario* (la parte pública de un par de clave pública/privada)
- Nombre de Usuario (este nombre suele ser otro *Atributo* de *Identidad*)
- Fortaleza/confianza de la credencial
- Declaraciones de Ubicación; dirección IP, geolocalización, GPS, Localización Móvil
- *Identidad Organizativa* (*Identificador* – criptográfico) y declaraciones organizativas
- *Identidad* de Dispositivo (*Identificador* – criptográfico) y declaraciones de dispositivo; funcionalidad solicitada, funcionalidad ofrecida, capacidades Sandbox, contenedor seguro, limpieza del dispositivo
- *Identidad* de Código (*Identificador* – criptográfico) y declaraciones de Código
- Registro/cumplimiento de capacitación, etc.

La fuente principal de *Identidad* y de *Atributos* de una *Identidad* (que puede provenir de una fuente diferente) debe ser identificada en el diseño del proceso de asignación de derechos.

Como regla, el servicio o aplicación debe evitar ser en sí mismo la fuente maestro de *Identidad* (las excepciones pueden ser un servicio de RRHH basado en *Cloud*, o un servicio *Cloud IDaaS*¹⁰⁰). Sin embargo, durante la transición a los servicios *Cloud* (no es la mejor práctica) el servicio / aplicación *Cloud* pueden necesitar identidades u operar en un modo mixto.

Todos los *Atributos* deberían estar asociados a una *Identidad*, ya que sin el *Identificador* asociado y el nivel de confianza con ese *Identificador*, los *Atributos* no tienen origen. A pesar de que a primera vista puede parecer poco intuitivo, la fortaleza en el proceso de asignación de derechos reside en definir esos *Atributos* como necesarios para que las reglas funcionen en la forma que el negocio requiere que lo hagan y por tanto identificar la fuente autoritativa (o lo más cerca posible) para proporcionar esos *Atributos* (con el *Identificador* asociado). Algunos ejemplos:

- Nivel de amenaza de Seguridad: Organizativa, Gubernamental, o *Identidad* proporcionada por un tercero
- Aprobaciones o decisiones previas realizadas por otras Entidades: *Identidad de Entidad*
- Calidad de Servicio o políticas de uso asociadas a un recurso objetivo protegido

¹⁰⁰ IDaaS, *Identity as a Service*. Ver capítulo 14.

12.6 El proceso de Asignación de Derechos (Entitlement Process)

El proceso de asignación de derechos comienza cuando el usuario convierte los requisitos de negocio y de seguridad en un conjunto de reglas de asignación de derechos. Este proceso definirá las *Identidades* y *Atributos* requeridos para ser capaz de evaluar adecuadamente las reglas autorizadas. El proceso de asignación de derechos y las reglas derivadas no deben solo manejar la gestión de autorización y acceso a un sistema *Cloud*, pueden especificar el grado de negociación/asignación en todas las capas de la infraestructura *Cloud*, por ejemplo, para permitir protocolos e interfaces en la capa de red y/o sistema.

El proceso debe estar incluido en cualquier documento de requisitos de negocio y también de requisitos técnicos; deberá ser una característica integral del proceso de aprovisionamiento/incorporación de clientes del CSP.

No termina una vez el servicio *Cloud* está listo y en ejecución, si no que las reglas de asignación de derechos y las subsiguientes que gestionan autorización y acceso deben ser objeto de revisión regular. El proceso debe ser auditado por el “propietario de sistemas” para verificar los requisitos de negocio. Cualquier auditoría debe incluir la valoración de riesgos y amenazas y los requisitos regulatorios.

Las soluciones actuales incluyen automatizaciones para convertir las políticas de alto nivel en reglas técnicas de acceso (bajo nivel), incluyendo:

- **Model-driven security**¹⁰¹, un proceso basado en herramientas para el modelado de requisitos de seguridad a alto nivel de abstracción y utilizando otras fuentes de información disponibles sobre el sistema (producidas por otros propietarios)
- Agrupación de reglas técnicas de acceso en grupo similares para reducir la complejidad
- Intentos de hacer las políticas técnicas más fáciles de entender

El proceso de asignación de derechos o Entitlement debe definir aquellas *Entidades*, *Identidades* y *Atributos* que se requieren para tomar decisiones significativas de autorización y acceso. Debe definir también aquellos *Atributos* que son fijos en el proceso, o lo que tienen un aspecto temporal (cambia con el tiempo) del mismo, y por tanto cualquiera que sea el intervalo de tiempo al que deban ser revalidados, o el disparador dentro del proceso, forzarán la revalidación.

Donde se definen en el proceso de asignación de derechos Identidad y Atributos cuyo origen está fuera del control del negocio, la *Identidad* Organizativa de ese proveedor (Entidad) debe ser incluido también, y de esta manera (en algún momento en el tiempo) excluirlo.

Típicamente las reglas de asignación de derechos se interpretan en uno de estos tres puntos:

1. Utilizando un punto de Refuerzo e Políticas central/externo o Policy Server o Policy-as-a-Service
2. Incluido con parte de la aplicación *Cloud*
3. Usar identidad como servicio (*IdaaS*)

¹⁰¹ www.modeldrivensecurity.org

12.7 Gestión de Acceso y Autorización

La gestión de Acceso y Autorización es el proceso por el que las reglas de asignación de permisos se convierten (mediante la capa de Autorización) en reglas de Gestión de Acceso,

En la mayoría de los sistemas basados en *Cloud*, la capa de Autorización es parecida a un “*Policy Decision Point*” (**PDP**)¹⁰² (o el punto que evalúa y emite decisiones de autorización, y la capa de Gestión de Acceso, el “*Policy Enforcement Point*” (**PEP**)¹⁰³, el punto que refuerza las decisiones de PDP.

El PDP y PEP serán parte del ecosistema de autorización que utilice uses **XACML**¹⁰⁴ (*eXtensible Access Control Markup Language*) como lenguaje declarativo de control de acceso implantado en XML.

Un modelo PEP podría ser algo tan sencillo como una comparación SI (condicional) en el servicio *Cloud*, o tan complejo como un agente específico en el servidor de aplicaciones o un filtro ad-hoc en un proxy XML que intercepte peticiones de acceso, recupera los datos necesarios (atributos de usuario) para verificar los permisos aplicables, y a continuación, tome las decisiones adecuadas.

No se trata de forzar el uso de **XACML**, **PDPs**, y **PEPs** en un entorno *Cloud*, ya que la funcionalidad puede implantarse potencialmente de otras formas (probablemente en un ecosistema cerrado o propietario).

Los PDP pueden implantarse fuera del entorno *Cloud*, posiblemente dentro del entorno del cliente. Esto puede tener un número de ventajas potenciales como interactuar con el DS interno y/o la posibilidad de integrar logs de decisión directamente en los sistemas internos de registro,

12.8 Arquitecturas de Interfaz con Proveedores de Identidad y Atributos

Existen tres arquitecturas básicas de interactuar con proveedores de *Identidad y Atributos*:

1. Un modelo “*hub-and-spoke*” donde *Identidad y Atributos* se gestionan centralizadamente (coordinado) por el hub, el cual entonces interactúa con el servicio(s) o aplicación(es) *Cloud*
2. El modelo libre-de-forma donde la aplicación y/o servicio *Cloud* pueden ser configurados para aceptar *Identidad y Atributos* de múltiples orígenes.
3. La solución híbrida, donde los componentes están distribuidos, potencialmente utilizando otros servicios *Cloud*.

Cada modelo tiene sus méritos, y la elección se basará en el número de factores, incluyendo:

- Donde los clientes para el servicio tengan su identidad
- La habilidad del servicio *Cloud* elegido
- La habilidad de la empresa de proporcionar *Identidad y Atributos* bien declarados.

¹⁰² **PDP** - Policy Decision Point

¹⁰³ **PEP** - Policy Enforcement Point

¹⁰⁴ **XACML** - eXtensible Access Control Markup Language

12.8.1 Modelo "Hub and Spoke"

El enfoque "hub and spoke" permite al servicio *Cloud* interactuar directamente con la organización para su información *Identidad y Atributos*, idealmente en forma de protocolos de declaración basados en estándares, como *OAuth* y *SAML*.

Los sistemas internos de la organización son responsables de mantener el registro de los usuarios, otras entidades y los Atributos. Este sería un sistema más parecido al tradicional IAM (GIA), y de esta manera probablemente la transición más sencilla para soluciones *Cloud* implantada por las organizaciones, ya que la mayoría de sistemas **DS** o **LDAP** pueden tener capacidad *SAML* incorporada.

Lo más probable en este modelo es que el proceso de asignación de derechos debería manejarse dentro de la organización mediante el uso de *Policy Enforcement Point* y *Policy Server* comunicándose vía *XACML* (si bien *XACML* no está ampliamente utilizado aun)

Un beneficio de este enfoque es que manteniendo un *Policy Enforcement Point* dentro de la organización permite la integración de logs de auditoría para ser mantenidos dentro de la organización e incluso correlacionados con otros registros de auditoría separados (fuera del entorno *Cloud*, o de otros entornos *Cloud*) para obtener el escenario completo. Como ejemplos, análisis de Segregación de Tareas y requisitos de satisfacción o legales.

El enfoque "hub-and-spoke" es probable que sea utilizado cuando se necesita un alto grado de control sobre todos los "usuarios" con un proceso de asignación de derechos central. Más probable en organizaciones que están sujetas a una regulación intensa. El "hub-and-spoke" también reduce la dependencia en los proveedores de *Identidad/Atributos*, ya que los Atributos se almacenan frecuentemente (duplicados) dentro del hub central.

Es también el modelo utilizado en organizaciones suscritas al "Bridge" o "Identity Hub."

12.8.2 Free Form Model

En el modelo "free-form", el servicio / aplicación *Cloud* es responsable de mantener los orígenes de *Identidad y Atributos*. Esta solución es más adecuada para una solución orientada al público o una solución con un gran número de distintos participantes.

Este enfoque tiene la ventaja de que se más sencillo de instalar, al menos con los protocolos actuales de federación (como es *SAML*) pero depende de una buena implantación del modelo de asignación de derechos para permitir que escale a un gran número de "usuarios"

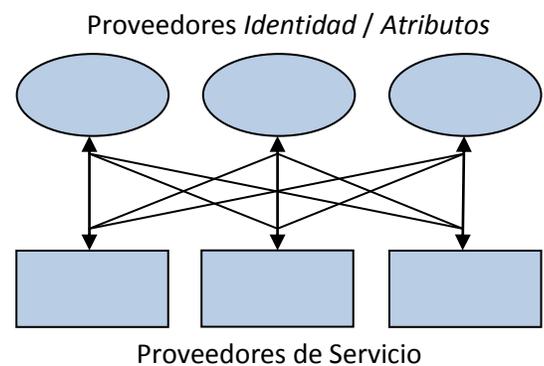


Figura 16—Modelo "Free Form"

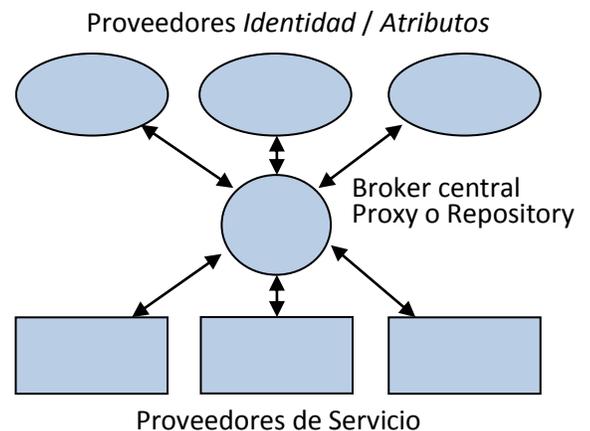


Figura 15—Modelo "Hub & Spoke"

Una posibilidad es instalar una relación de confianza federada punto-a punto (utilizando protocolos como SAML y OAuth) entre el servicio y los proveedores de *Identidad y Atributos*, pero este enfoque requiere un proceso eficiente para incluir y excluir a estos proveedores.

El modelo “*free-form*” plantea retos de aprovisionamiento de “usuarios”, ya que el entorno de nuevas entidades conectándose es más probable de ser más ad-hoc. De nuevo, un diseño cuidadoso del Proceso de Asignación de Usuarios ayudara a aliviar el problema. La Figura 16 arriba ilustra el enfoque punto-a punto.

12.8.3 Modelo Híbrido

El modelo híbrido es (por definición) una mezcla de los dos anteriores. Por ejemplo, las reglas de asignación de derechos pueden residir dentro de la organización y meterlas en un **PDP**, el cual en si mismo es un servicio *Cloud*, y entonces esas decisiones se entregan a múltiples distintos PEP que son parte de servicios *Cloud* diferentes. En despliegues a gran escala, pueden existir varios servidores de políticas federados que dan servicio a muchos PDP/PEP distintos. El modelo híbrido se podrá encontrar también en organizaciones que mezclan la computación tradicional y/o heredada con un (publico y/o privado) entorno *Cloud*.

Este modelo puede ofrecer un uso eficiente de los recursos distribuidos, pero sus riesgos se vuelven complejos con la aparición de posibles lagunas legales. Esto hace el mantenimiento a largo plazo mas problemático (el razonamiento de reglas simples es mas fácil de entender cuando los que las implementaron ya no están).

El modelo híbrido también plantea relativas a cuestiones de decisión de registro y toma de acciones con la necesidad potencial de aunar todos los logs en un punto único en un formato común que permita una visión holística.

La complejidad potencial del modelo híbrido enfatiza la necesidad de ser capaz de utilizar herramientas de visualización para desarrollar, mantener, y auditar la traducción de las Reglas de Asignación de Derechos en control de acceso.

12.9 Niveles de Confianza con Identidades y Atributos

La *Identidad* y los *Atributos* aparecen con muchos niveles de confianza, en las diferentes identidades utilizadas en una transacción y con los Atributos unidos a esas identidades. Tradicionalmente esta falta de confianza ha conducido a las organizaciones a tener que mantener identidades para cada uno que necesite acceso a sus sistemas, lo cual puede ser (en algunos casos) para cientos de miles de personas a los que no emplean o gestionan directamente.

Algunas organizaciones (militar/aeroespacial, farmacéutica, etc.) que necesitan colaborar con un nivel de confianza pre acordado, utilizan un “*Bridge*” o “*Federation Hub*” (ver sección 12.4), donde las identidades confiables también tienen *Atributos* confiables asociados.

Durante el proceso de asignación de derechos es esencial comprende que no solo los Atributos requeridos, si no también el origen de esos Atributos, deben ser proporcionados por la organización, y la Fortaleza (nivel de confianza) con los que deben ser declarados.

Para aceptar Atributos de una organización externa con un nivel de confianza definido exigirá un proceso de inclusión para esa organización, y la Identidad (Identificador) de la organización que declarará esos Atributos.

Como norma, el objetivo deberá ser obtener Identidad y Atributos de la fuente principal / autoritativa de esos Atributos teniendo una Identidad conocida declarándolos, ya que el nivel de confianza que puede depositarse en el Atributo no puede exceder el nivel de confianza depositado en la Identidad que lo declara.

Donde los Atributos sean declarados unívocamente dentro del propio sistema *Cloud*, entonces debe establecerse un proceso de gobierno para asegurar que todos los Atributos son exactos y tienen una gestión de ciclo de vida apropiada.

12.10 Aprovisionamiento de Cuentas en Sistemas Cloud

Cuando es necesario aprovisionar una “cuenta” en sistemas *Cloud* (típicamente para un usuario, pero podría ser para un tipo *Entity*) aparecen ciertos retos en el momento de provisionar (y des-provisionar) estas cuentas, ya que el modelo normal “*push*” utilizado en las organizaciones no es una solución generalmente viable para una implementación en *Cloud*.

En el momento de redactarse esta guía, no existen estándares de aprovisionamiento de-facto o ampliamente utilizados; **SPML**¹⁰⁵ (Service Provisioning Markup Language) no ha sido ampliamente adoptado por los proveedores de *Cloud*, y **SCIM** (*Simple Cloud Identity Management*) está comenzando a emerger como un estándar potencial.

La clave para aprovisionar entidades en un sistema *Cloud* es comprender completamente la gestión del ciclo de vida de una cuenta, desde la creación, gestión, y eventualmente desmantelamiento (incluido borrado y/o archivado) a lo largo del sistema que tanto proporciona como consume la *Identidad y Atributos*.

Existen algunos puntos claves que deben abordarse como orígenes de *Identidad y Atributos* en materia de aprovisionamiento:

- El enlace con Recursos Humanos (o la fuente autoritativa de información de usuario-persona) es problemático ya que a menudo RRHH solamente es fuente principal en cuestiones de nomina.
- Normalmente no existen fuentes autoritativas de información para socios o terceros y sus dispositivos.
- La capacidad de aprovisionar otras entidades (particularmente organizaciones y dispositivos) no existe en muchas organizaciones.
- Los servicios públicos de identidades generalmente solo proporcionan *identidad* auto-declarada y solo sobre personas; no se extiende a otros tipos de *Entidad*.
- El desaprovisionamiento necesita extenderse a todas las entidades, de no ser así, la mayoría de organizaciones no tienen la capacidad de escindir otra organización cuando finaliza un contrato o revocar el código que está operando en los sistemas cuando está obsoleto o defectuoso.

Estos temas y la inmadurez de los estándares de aprovisionamiento acentúan la necesidad de una buena planificación y un enfoque holístico hacia como *Identidad, Atributos*, cuentas, y la gestión del ciclo de vida de todos los tipos *Entidad* operaran en el ecosistema *Cloud* que se esté desplegando.

¹⁰⁵ **SPML** - Service Provisioning Markup Language

12.11 Identity-as-a-Service (Identidad como Servicio)

*Cloud Identity as a Service (IDaaS)*¹⁰⁶ es un término amplio que cubre la gestión de cualquier parte de la *Identidad*, *Entitlement* (asignación de derechos), y la gestión de Autorización/Acceso en el servicio *Cloud*.

Esto abarca dar servicio para software, plataforma o servicios de infraestructura, y para ambas *Clouds*, públicas y privadas. Las soluciones híbridas también son posibles, de forma que las identidades pueden seguir gestionándose internamente dentro de una organización, mientras otros componentes como la autenticación se externalizan a través de (SOA)¹⁰⁷ *Service Oriented Architecture*. Sea crea efectivamente una capa de Plataforma como Servicio (PaaS) para facilitar una solución IAM (Gestión de Identidades y Accesos) basada en *Cloud*.

Para más información consúltese la sección que cubre “Identity-as-a-Service” en el Dominio 14 - “Security-as-a-Service”.

12.12 Cumplimiento y Auditoria

Los resultados de las reglas de “*entitlement*” (asignación de derechos) podría ser muy necesario registrarlos junto con las decisiones asumidas por las reglas/procesos de autorización por razones de cumplimiento o seguridad. Ambos están íntegramente unidos a la *Identidad*. Sin una gestión adecuada de la Identidad, no hay forma de garantizar el cumplimiento regulatorio. La auditoria también requiere una gestión adecuada de la Identidad, y el uso de los ficheros de “log” tiene poco valor sin un sistema de *Identidad* adecuado.

12.13 Diseño de Aplicaciones para la Identidad

Esta sección se refiere exactamente al diseño de aplicaciones en lo que a Identidad se refiere y debería leerse conjuntamente con el Dominio 10 – Seguridad en Aplicaciones.

El diseño de Sistemas o aplicaciones basadas en *Cloud* requiere un cambio de mentalidad cuando se trata de Identidad como “información y *Atributos*” que será consumida por el servicio o aplicación *Cloud*, debiendo mantenerse por lo menos durante la transacción, y probablemente más allá en alguna facetas; pero ya que es probable que el entorno *Cloud* no sea parte de la jurisdicción física o lógica de una organización, y puede incluso estar en jurisdicciones legales diferentes, el diseño del servicio y aplicación necesitaran ser sustancialmente diferentes que las prácticas utilizadas en el entorno cliente servidor en una DMZ propietaria y gestionada por la organización.

El objetivo del diseño debería minimizar la necesidad de *Identidad* y *Atributos*. Cuando sea posible, comenzar desde el principio de que la identificación no es necesaria hasta un punto que marque el cambio de la provisión de cuentas de un uso a una cuenta de usuario “identificada”. Ejemplos:

- Se pueden establecer sesiones únicas utilizando otros *Atributos*. Por ejemplo la dirección IP del dispositivo en conexión (entendiendo que esa IP podría ser suplantada) o a una cookie de sesión única.

¹⁰⁶ IDaaS - Cloud *Identity* as a Service

¹⁰⁷ SOA - Service Oriented Architecture

- En muchos casos el “*entitlement*” basado en *Atributos* solamente sería adecuado sin necesidad de información de usuario o una Identidad real; no asumamos que una *Persona* tiene que vincularse con una sesión o incluso una cuenta.
- En el momento de encontrar una nueva Entidad por vez primera (digamos autenticándose mediante SAML) entonces se crea una cuenta básica de un uso [Nótese que este enfoque requiere des-aprovisionamiento]
- Utilizar derivación de *Atributos* cuando sea posible, (por ejemplo, no preguntar por la fecha de nacimiento, en su lugar preguntar “si es mayor de 18” [si FechaNacimiento > (hoy – 18 años)])

Cuando se generen cuentas únicas, debe decidirse si el sistema consumirá un *Identificador* externo único de la *Entidad* o si generara su propio *Identificador* único (como un numero de referencia de cliente).

Debe prestarse una cuidadosa atención en los sistemas *Cloud* que mantienen cuentas de usuario. Debe hacerse un diseño cuidadoso en cómo las cuentas de usuario *Cloud* se sincronizarán con cuentas de usuario existentes en otros sistemas (ya sea *Cloud* interna o externa), particularmente en torno a la integración con procesos de “*joiners and leavers*” (entrantes y salientes en términos de acceso), y los cambios que las personas requieren en sus movimientos internos. El diseño de un sistema *Cloud* que escale (un ejemplo serian 100.000 usuarios con un nombre de usuario no conectado y/o password no sincronizada) requiere evitar forzar procesos comunes de atención a usuarios, incluyendo scripts de sincronización manuales o semiautomáticos, procesos de validación de fortaleza de contraseñas, de restablecimiento de contraseñas, restablecimiento por compromiso de la contraseña, etc. todo ello debido a una falta de diseño inicial en relación al consumo de identidades externas.

Evítese intentar extender un DS interno en el servicio *Cloud* y/o replicar el DS e la organización en Internet (generalmente muy inseguro) o a través de un “*back-channel*” (línea dedicada o VPN) ya que expone completamente el DS la organización en un entorno que la organización no controla. También seamos cautelosos con las promesas de los productos RSO (*Reduced-Sign-On*) ya que generalmente funcionan comprometiendo la seguridad de *logon* internamente, mucho más cuando se intenta extender RSO a un entorno *Cloud*.

Como regla, los Servicios *Cloud*, e incluso las aplicaciones *Cloud*, aceptaran los formatos estándar de federación SSO como SAML y OAuth (o incluso el menos aceptado *WS-Federation*)

Cuando se diseñe una aplicación para consumir *Identidad* y *Atributos*, recordemos que Identidad abarca todas las Entidades, y que la seguridad de aplicación será, donde sea posible, parte de un enfoque holístico que incluye todas las capas; la capa de Red, de Sistema, de Aplicación, de Proceso, y la capa de Datos (según se detalla en la sección 12.3). Una aplicación podría (por ejemplo) ofrecer dos métodos de conexión: una conexión completa usando Web/AJAX/Java o una conexión “pantalla capturada” de tipo *Citrix* con el tipo de conexión permitida determinada por las Reglas de “*Entitlement*” (definidas en el proceso asociado).

12.14 Protección de la Identidad y Datos

Una cuestión a tener en cuenta en todas las organizaciones es manejar aspectos de una *Identidad* que comprende información personal, *Personal Identifiable Information (PII)*, y especialmente la información clasificada como sensible,

SPI¹⁰⁸. Los servicios *Cloud* gestionados o ubicados fuera de la organización necesitarán supervisión especializada para asegurar que toda la legislación y regulación aplicable se está teniendo en cuenta.

Para tener en cuenta que leyes o reglamentos se tienen que considerar, debe comenzarse por una lista de este tipo (no es exhaustiva):

- Todos los países objeto de los datos
- El país donde opera la organización
- Países donde la organización tiene presencia oficial
- Países en los que la organización cotiza o comercializa algún tipo de participación o acciones.
- El país o países donde los servicios *Cloud* están físicamente ubicados
- La legislación relevante, reglamentos, y pseudo reglamentos (como PCI-DSS)

12.15 “Consumerización” y el reto de la Identidad

La interacción con los clientes y/o sus dispositivos conlleva una serie de retos y oportunidades en los servicios y aplicaciones basadas en *Cloud*. La habilidad del cliente y sus dispositivos para interactuar directamente con un servicio *Cloud* basado en Internet elimina una capa de complejidad de red pero introduce una serie de retos que pueden mitigarse potencialmente usando *Identidad*.

Sin embargo, en la parte del cliente, los estándares de *Identidad* de usuario y dispositivo están fragmentados y (por definición) pocas veces tendrán el mismo nivel de conformidad y estandarización que pueden conseguirse en un entorno corporativo.

Desafortunadamente, muchos dispositivos de clientes y los clientes mismos no tienen una forma sencilla o estándar de registrarse en un sistema de autenticación que proporcione autenticación fuerte, y así, autorizar sin una *Identidad* fuerte es difícil. Incluso cuando los usuarios disponen de un método de autenticación fuerte (por ejemplo con su banco) para una cuenta de usuario, este casi nunca puede ser reutilizado para otra cuenta/proveedor. Esto resulta en una situación donde la *Identidad* para el cliente ha traspasado ya los límites de la escalabilidad. Más del 61 por ciento de la gente usa la misma contraseña siempre que pueden¹⁰⁹; esto conlleva que cada registro o autenticación adicional conlleve una pérdida de clientes.

Resolver este problema con un acceso continuo a las aplicaciones facilitaría los criterios de negocio, y una clara separación entre *Identidad* y autorización facilitaría usos adicionales, por ejemplo permitiendo a un individuo delegar el uso de su *Persona* vinculado a una tarjeta de crédito específica en nombre de transacciones de terceros.

12.16 Proveedores de Servicios de Identidad

El consumo de información sobre la *Identidad* de un servicio externo tiene sus propios retos. Un par de ejemplos pueden ser los niveles de confianza en la organización proveedora y la validación de los Atributos. La mayoría de las propuestas actuales o las ofertas completas y consistentes de una infraestructura de Identidad son extrapolaciones de las

¹⁰⁸ SPI - Sensitive Personal Information

¹⁰⁹ <http://www.guardian.co.uk/technology/2008/jan/17/security.banks>

necesidades de un único o un grupo de participantes con limitado o ningún conocimiento de las necesidades de otras comunidades.

Casi todos los servicios abiertos/públicos de Identidad solo tratan la verificación de usuario. Los que ofrecen información personal (*Atributos* además de *Identidad*) lo hacen utilizando *Atributos* que son o bien auto-declarada o de una fuente no autoritativa.

Algunos ejemplos de Fuentes de *Identidad* y *Atributos* son:

- Gobiernos Nacionales
 - Estados Unidos, NSTIC – solo estrategia
 - Alemania “*EID card*,” Austria “*Citizen Card*,” Estonia “*ID Card*,” España “*dniE*,” Finlandia “*Citizen Certificate*,” Hong Kong “*Smart ID Card*,” Malasia “*MyCad*”
- Públicos – integración via APIs
 - Facebook
 - Amazon
 - Google
 - Microsoft Passport (Windows Live ID)
 - OpenID providers (Varios)
 - Twitter
- Bridges¹¹⁰ o “Hubs”
 - *Research / Education Bridge (REBCA¹¹¹)*, da servicios al sector educativo universitario norteamericano
 - *Federal PKI Architecture (Federal Bridge)* da servicio a las agencias federales norteamericanas.
 - *CertiPath/Transglobal Secure Collaboration Program¹¹²*, da servicio a las industrias aeroespaciales y de defensa.
- *SAFE-BioPharma Association¹¹³*, da servicio a la industria bio-farmacéutica y de salud.
- Servicios de *Identidad*
 - Comprobación / validación de código postal y dirección (varios)
 - Experian / Equifax

¹¹⁰ www.the4bf.com

¹¹¹ www.hebca.org

¹¹² www.certipath.com / www.tscp.org/

¹¹³ www.safe-biopharma.org/

- Verificación 3D card (Visa/MasterCard)
- eBay / PayPal / X.Commerce

12.17 Recomendaciones

12.17.1 Recomendaciones para Federación

- Clientes, implantadores, y proveedores deben acordar el contexto y definición de “federación” que va a utilizarse.
- Los implantadores deben comprender la existencia de una relación de confianza y confianza transitiva y la necesidad bidireccional de las mismas.
- Deben, dense sea posible, utilizar federación basada en estándares abiertos como SAML y OAuth.
- Si se utiliza en “*Bridge*” o “*Federation Hub*”, los implantadores deben comprender la naturaleza y relación de las confianzas que existen entre los distintos miembros. Entendiendo que lo que podría significar para tus reglas de “*entitlement*” si existe otro miembro registrado en el *Cloud* o realizando federación con otro bridge.
- Los implantadores deben tener en cuenta que los proveedores de *Identidad* publica como Facebook, Yahoo, o Google proporcionan una fuente de (normalmente de bajo nivel y auto-declarada) *Identidad* que no garantiza que no vayan a realizar federación con otros proveedores en el futuro.
- No deben tenerse en cuenta ejemplos de mal diseño de soluciones para obtener *Identidad* de un DS conectado a un sistema de gestión de acceso de una solución *Cloud*. Tales ejemplos incluyen VPN y líneas dedicadas.

12.17.2 Recomendaciones de Aprovisionamiento y Gobierno

- Todos los *Atributos* deben tener su origen de una fuente lo mas cercana posible a la autoritativa/principal.
- Como regla, el servicio *Cloud* o la aplicación en si misma deberían evitar ser la fuente principal para la *Identidad*.
- El servicio *Cloud* o la aplicación en si misma deberían ser solamente la fuente principal de los *Atributos* que controlan directamente.
- Todos los *Atributos* empleados en este proceso deberían tener un nivel de confianza conocido.
- Todos los *Atributos* consumidos deberían estar enlazados a una *Identidad*.
- El *Identificador* de una *Entidad* definida debería firmar todos los *Atributos* consumidos.
- Cada *Atributo* debería tener un ciclo de vida adecuado a su propósito.
- Cada *Atributo* (y su *Identificador* relacionado) deberá tener un ciclo de vida adecuado a su propósito

12.17.3 Recomendaciones de Asignación de derechos (concesión de autorización)

- Todas las partes en el proceso de asignación de derechos (definición) deben ser claramente identificadas.
- Deben existir responsabilidades claramente definidas para la aprobación y terminación de reglas de *entitlement*.
- Debe definirse claramente un proceso para gestionar cambios en las reglas de asignación de derechos.
- Debe definirse una frecuencia (o un evento desencadenante) para auditar las Reglas de Asignación de derechos.
- El proceso de asignación de derechos debería enfocarse en producir Reglas que sean simples y mínimas, y diseñadas usando el principio de mínimo privilegio.
- El proceso de asignación de derechos debería enfocarse en producir Reglas que minimicen la exposición de la Identidad o eviten totalmente la necesidad de consumirla.
- Los *Atributos* que son temporales (como la geolocalización) necesitan comprobación en tiempo real a través de un ciclo de vida de transacción para revalidar las reglas de asignación de derechos.
- Las reglas de asignación de derechos deben dispararse mediante un proceso (o intento de iniciar un proceso, como una transferencia financiera fuera del entorno). En algunos entornos, las mejores prácticas en reglas de asignación de derechos deberían ser deshabilitar tales funciones. En otros, requerirían Identidad o Atributos adicionales en el punto de ejecución para asegurar que la *Entidad* dispone de autorización a realizar el proceso.
- Los implantadores deberán asegurar las confianzas bidireccionales para garantizar las relaciones seguras óptimas para la transacción. El proceso de asignación de derechos debe definir esto.
- El diseño de reglas de asignación de derechos debe incluir delegación¹¹⁴ de acceso mediante una Entidad secundaria a alguna, pero no necesariamente a toda, información a la que la Entidad primaria puede acceder.
- El diseño de la asignación de derechos debería incluir la detención del acceso (incluida la detención legal), aunque el diseñador de las reglas de asignación de derechos necesitara tener en cuenta la jurisdicción del sistema, organización y las entidades implicadas. Debe solicitarse asistencia legal antes de implementar ninguna regla de detención de acceso.
- Deberán usarse, donde sea práctico, interfaces de gestión, herramientas, u otras tecnologías de visualización para ayudar en la gestión de Asignación de derechos y para asegurar la interpretación cumple los requisitos legales y/o regulatorios (por ejemplo, segregación de tareas en SOX).

12.17.4 Recomendaciones de Autorización y Acceso

- Los implantadores deben asegurarse que los Servicios disponen de una función importar/exportar dentro de estándares como OASIS XACML.

¹¹⁴ La delegación está recientemente soportada en XACML 3.0

- En el uso de PDP en un entorno *Cloud*, los implantadores deben tener en cuenta como se puede extraer y/o integrar el *logging* de autorización en un sistema general registro (logs) de una organización para tener una visión holística del acceso.
- Deben asegurarse que los servicios existentes (*legacy*) pueden interactuar con PEP/PDP.
- Igualmente, debe asegurarse que cualquier PDP sea adecuado para interpretar las reglas definidas en el proceso de asignación de derechos.
- Y deben considerar el uso de “política-como-servicio” si es necesario que exista un servidor centra de políticas (por ejemplo para *Cloud mash-up*).

12.17.5 Recomendaciones de Arquitectura

- Los implantadores deben asegurarse que los proveedores de *Cloud* ofrecen PEPs/PDPs de gestión de autorización que pueden configurarse con reglas de asignación de derechos.
- Todos los componentes de la *Identidad*, Asignación de derechos, y gestión de Autorización/Acceso (IdEA) trabajan correctamente en conjunto.
- Que los *Policy Decision/Enforcement Points* (PEPs/PDPs) utilizan protocolos estándar (como XACML) y evitan (o ignoran) protocolos propietarios (como “web services” directos u otras llamadas a middleware).
- Los Servicios de autenticación fuerte cumplen con **OATH**. Con una solución compatible OATH, las organizaciones pueden evitar el “*lock*” mediante las credenciales de autenticación de un proveedor.
- Los Servicios y aplicaciones *Cloud* deben soportar la capacidad de consumir autenticación de una Fuente autoritativa mediante SAML.
- Los servicios disponen de una función importar/exportar dentro de estándares como OASIS XACML.
- Los servicios pueden interactuar con los PEP/PDPs instalados en la infraestructura *Cloud* y con los Puntos de Monitorización de Políticas (*Policy Monitoring Points*) para la monitorización/auditoria de incidentes.
- El log de las decisiones de autorización y acceso realmente concedidos puede registrarse en un formato común utilizando protocolos seguros estándar.

12.17.6 Recomendaciones de Asignación de derechos

- Los implantadores deben asegurar que cada *Identidad* y *Atributo* definido en el proceso de asignación de derechos encaja con el nivel de confianza necesario (o es aceptable) tanto en la *Identidad/Atributo* en sí mismo como la fuente que lo proporciona.
- Asegurar que todas las Fuentes de *Identidad/Atributo* proporcionan *Identidad* de la organización.
- Los *Atributos* se validan en una fuente maestra cuando sea posible, o lo más cercano posible.

- La utilización de *Atributos* lleva a la conclusión correcta. (El contexto puede ser diferente del originador de los *Atributos*).
- La fuente de *Identidad/Atributo* dispone de los estándares de calidad y los mecanismos de gobierno que cumplen con las necesidades.
- Los clientes deben ser conscientes que la confianza basada en la reputación puede ser una fuente importante de confianza. Mediante la definición de asignación de derechos, serán conscientes de que las transacciones de pequeño valor incrementan la confianza transaccional, que podría verse comprometida en transacciones mayores posteriores.

12.17.7 Recomendaciones de Aprovisionamiento

- Los proveedores deben ser conscientes de si SPML o SCIM pueden ser una opción viable para el aprovisionamiento
- Los implantadores seguirán la regla de menor privilegio al aprovisionar una cuenta. En el caso de entidades como dispositivos, sería deseable un enlace a un registro de activos de la organización.
- La mayoría de sistemas y aplicaciones tienen una relación uno a uno entre el usuario y el acceso sin un concepto de delegación.
- Los implantadores deben asegurarse que el aprovisionamiento y des-aprovisionamiento no se limitan a las entidades de usuario. Las arquitecturas deben incluir la autorización para todos los tipos de *Entidad*.
- El aprovisionamiento y des-aprovisionamiento se realizan en tiempo real.
- Los proveedores deben asegurar la criticidad del mantenimiento de *Identidad* and *Atributos* para mantener la exactitud del asignación de derechos.

12.17.8 Recomendaciones para Cumplimiento y Auditoria de Identidades

- Los implantadores se aseguran que los logs relativos a las reglas de asignación de derechos rules / procesos de autorización pueden estar disponibles.
- Donde sea necesario que los logs se integren en un sistema mayor (posiblemente remoto, como ejemplo un sistema de detección de fraude o de análisis de segregación de tareas) se garantice que la disponibilidad, actualización, formato y seguridad de la transmisión del log son las adecuadas.
- Cuando se registren las decisiones de acceso, los Atributos se agruparan con la lógica de asignación de derechos utilizada en tiempo de decisión, y el resultado debe registrarse.
- Los *Atributos* de un componente temporal necesitarían ser revalidados, y por tanto registrados de nuevo, durante el tiempo de vida de la sesión.
- Al registrar PII o SPI entonces, cuando sea posible, deben utilizarse derivación de *Atributos* para minimizar la exposición PII o SPI en los logs.

- Los clientes deben ser conscientes que los logs que contienen PII o SPI son susceptibles de ser objeto de las leyes de protección de datos.

12.17.9 Recomendaciones para el Diseño de Aplicaciones

- Los implantadores deben utilizar ITU X.805 / definición de 3-capas de Usuario, Sistema y Gestión para garantizar la segregación.
- Minimizar la necesidad de *Identidad* y *Atributos* en el diseño de aplicaciones.
- Cuando sea posible, diseñar Sistemas *Cloud* que consuman *Identidad* y *Atributos* de fuentes externas.
- Los Sistemas *Cloud* soportan formatos estándar de SSO como SAML y OAuth.
- Adoptar un enfoque holístico de la seguridad, utilizando *Identidad* y *Atributos* a través de todas las capas del sistema.
- La autenticación mutua es crítica en todos los niveles, e incluso más importante en entornos *Cloud*, ya que el entorno *Cloud* necesita de entidades y otros sistemas para autenticarse, deberá por tanto ser capaz de autenticar a otros a cambio.

12.17.10 Recomendaciones para Protección de Datos

- Los implantadores minimizaran el uso y almacenamiento de PII o SPI. Se hará en la fase de diseño del proceso de para asegurar que se utilizan solamente las Identidades y Atributos esenciales.
- Se considerarán las siguientes tecnologías para minimizar la exposición de PII o SPI:
 - Cifrado
 - Uso de *Tokens*
 - Cifrado Homomórfico¹¹⁵

Para mayor información refiérase al Dominio 11 “Encriptación y Gestión de Claves”.

- Enfoques basados en las mejores prácticas para proteger SPI como el uso de clave dual, una en posesión del sujeto (o requerida en el log-in), y otra por el sistema para su uso en el procesamiento.
- El acceso del administrador PII y SPI debe ser detenido o restringido.
- Entender cómo una solicitud “**ARCO o Subject Access Request**”¹¹⁶ puede resolverse en el marco de tiempo legal requerido especialmente cuando los datos pueden estar alojados en un sistema *Cloud* no propietario / gestionado por la organización que recibe la petición.

¹¹⁵ En el momento de la redacción, la encriptación Homomórfica se encuentra en las primeras etapas de implementación.

¹¹⁶ “ARCO” En España, formulario de “Acceso, Rectificación, Cancelación y Oposición”. “Subject Access Request” derecho legal en algunos países para solicitar cualquier PII o SPI con datos del solicitante.

- Los clientes deben comprender que, si existe la necesidad de compartir PII o SPI, cómo debe obtenerse la aprobación del sujeto objeto de PII/SPI.
- Los implantadores deberán reducir los PII/SPI almacenados, particularmente cuando no sea la fuente autoritativa, y referenciar solamente aquellos atribuidos desde la fuente autoritativa en lugar de almacenarlos (y mantenerlos).
- Tendrán en cuenta los procesos por los cuales el mantenimiento PII/SPI (ya sea *Identidad* o *Atributos*) se maneja de la forma apropiada.

12.17.11 Recomendaciones para la Implementación de la Identidad

- Los implantadores deben comenzar utilizando el principio de la reutilización de la *Identidad* en lugar de asignar cada vez un registro nuevo a usuarios y/o dispositivos.
- Los clientes deben entender donde las fuentes existentes de *Identidad* pueden proporcionar niveles suficientes de confianza y ser reutilizadas.
- Los proveedores comprenderán cuales atributos acerca del usuario y dispositivos pueden ser declarados en un nivel suficiente de confianza para la transacción en curso.
- Los clientes deberán asumir, cuando sea apropiado, transacciones de bajo riesgo ejecutadas con bajo nivel de autenticación. Y escalar la Identidad solamente cuando se incremente el valor /riesgo de la transacción.
- Los proveedores proporcionaran una evaluación crítica de la *Identidad* y *Atributos* necesarios durante el proceso de Asignación de derechos en lo relativo a clientes y sus dispositivos.
- Los proveedores deberían entender qué tecnologías deben ser usados desde equipos de usuario para mejorar los niveles de seguridad. En particular, las tecnologías que usadas en backend.
- Los clientes deberán entender donde no se llevara a cabo la gestión de sus dispositivos y el nivel de garantía que ello proporciona; desde ninguna a una buena garantía.
- Y entenderán donde reside el nivel de garantía y de responsabilidad legal que pudiera surgir con una transacción desde el dispositivo de un cliente.

12.18 Requisitos

- ✓ Los implantadores deben diseñar las capas comunes de servicio para que actúen de forma independiente y así posibilitar la eliminación de silos de aplicación sin sacrificar las políticas y procedimientos de seguridad de la información.
- ✓ Todos los actores en el *Cloud* respetaran la integridad de la cadena de suministro y las prácticas IAM (en español, GIA -Gestión de Identidades y Accesos) existentes. Deben respetarse los elementos como privacidad,

integridad y la capacidad de auditoría. La integridad de la Identidad y la auditoria deben preservarse al trasladar datos fuera de la organización y/o desacoplar una solución en arquitecturas de servicios web.

DOMINIO 13 //

VIRTUALIZACIÓN

La virtualización es uno de los elementos clave de las ofertas de *Cloud IaaS* y de los *Cloud* privados, y se utiliza también cada vez más en partes del *back-end* de los proveedores de *PaaS* y *SaaS*. La virtualización es también, naturalmente, una tecnología clave para los escritorios virtuales (*virtual desktop*), que se proporcionan desde *Cloud* privados o públicos.

Los beneficios de la virtualización son ampliamente conocidos, incluyendo *multi-tenancy*, una mejor utilización de los servidores y la consolidación de CPD¹¹⁷. Los proveedores *Cloud* pueden lograr una mejor economía de escala, lo que se traduce en mejores márgenes, y las empresas pueden utilizar la virtualización para reducir los gastos de capital en hardware de servidores, así como aumentar la eficiencia operativa.

Sin embargo, la virtualización trae consigo todos los problemas de seguridad del sistema operativo que se ejecuta virtualizado, junto con nuevos problemas de seguridad de la capa del *hipervisor*, así como las nuevas amenazas específicas de la virtualización, ataques inter-VM (*Virtual Machine*) y puntos ciegos, preocupaciones sobre el rendimiento derivadas del uso de la CPU y la memoria para seguridad y la complejidad de las operaciones por la proliferación de VM (*VM sprawl*) como un inhibidor de la seguridad. Los nuevos problemas como los *gaps* en el arranque, mezcla de datos (*data commingling*), la dificultad de cifrar imágenes de máquinas virtuales, y la destrucción de datos residuales están entrando en el foco de atención.

Introducción. Aunque hay diversas formas de virtualización, la más común con diferencia es la virtualización del sistema operativo, y ésta es el foco de este dominio, el cual cubre los aspectos de seguridad relacionados con esa virtualización:

- Bastionado de la máquina virtual hospedada
- Seguridad del hipervisor
- Ataques Inter-VM y puntos ciegos
- Preocupaciones sobre el rendimiento
- Complejidad operacional derivada de la proliferación de VM
- Gaps en el arranque
- Cifrado de máquinas virtuales
- Mezcla de datos (*Data commingling*)
- Destrucción de datos de máquinas virtuales
- Manipulación de máquinas virtuales
- Migración de máquinas virtuales

La virtualización lleva consigo todas las preocupaciones de seguridad de los sistemas operativos alojados, junto con las nuevas amenazas específicas de la virtualización.

13.1 Dificultades de la arquitectura del Hipervisor

13.1.1 Bastionado de las VM alojadas

El apropiado bastionado y protección de una instancia de máquina virtual, incluyendo *firewall* (entrante/saliente), HIPS¹¹⁸, protección de aplicaciones web, antivirus, monitorización de integridad de archivos y de logs puede realizarse

¹¹⁷ CPD: Centro de Proceso de Datos (*Data Center*)

¹¹⁸ HIPS – *Host Intrusion Prevention System*

mediante software en cada cliente o utilizando una máquina virtual en línea en combinación con **APIs** basadas en el *hipervisor*.

13.1.2 Seguridad del *Hipervisor*

El *hipervisor* ha de ser bloqueado y bastionado utilizando las mejores prácticas. Las principales preocupaciones para las empresas y los usuarios de virtualización deberían ser la adecuada gestión de la configuración y las operaciones, así como la seguridad física del servidor que aloja el *hipervisor*.

13.1.3 Ataques Inter-VM puntos ciegos

La virtualización tiene un gran impacto en la seguridad de la red. Las máquinas virtuales pueden comunicarse entre sí a través de un hardware *backplane*, en lugar de una red. Como resultado, los controles de seguridad estándar basados en la red están ciegos a este tráfico y no pueden realizar la monitorización o el bloqueo en línea. Los *appliances* en línea virtuales pueden ayudar a resolver este problema; otro enfoque es la virtualización asistida por hardware, la cual requiere una integración a nivel API con los *hipervisores* y los entornos de gestión de la virtualización. La migración de máquinas virtuales es también un problema. Un escenario de ataque podría ser la migración de una máquina virtual maliciosa a una zona de confianza, y con los tradicionales controles de seguridad basados en la red, su mal comportamiento no sería detectado. Instalar un conjunto completo de herramientas de seguridad en cada máquina virtual individual es otro método para añadir una capa de protección.

13.1.4 Problemas de rendimiento

La instalación de software de seguridad diseñado para servidores físicos en un servidor virtualizado puede resultar en una degradación severa en el rendimiento, ya que algunas tareas de seguridad como la exploración antivirus son intensivas en uso de la CPU. El entorno compartido en servidores virtualizados requiere contenerse en el uso de recursos. El software de seguridad, especialmente con los escritorios virtuales o entornos de alta densidad, tiene que ser consciente de la virtualización o que necesita realizar las funciones de seguridad en una sola máquina virtual para dar soporte a otras máquinas virtuales.

13.1.5 Complejidad operacional por proliferación de VM

La facilidad con que puede provisionarse VM ha llevado a un aumento en el número de solicitudes de VM en las empresas de hoy en día. Esto crea una superficie de ataque más grande y aumenta las probabilidades de que una mala configuración o de que un error de operador abra un agujero de seguridad. La gestión basada en políticas y el uso de un marco de gestión de la virtualización es crítica.

13.1.6 Gaps en el arranque

La facilidad con la que una máquina virtual puede ser parada o arrancada, junto con la velocidad a la que cambian las amenazas, crea una situación donde una máquina virtual puede estar configurada de forma segura cuando es apagada, pero en el momento en que se inicia de nuevo, las amenazas han evolucionado, dejando a la máquina vulnerable. Las

mejores prácticas incluyen la seguridad basada en red y el "parcheo virtual" que inspecciona el tráfico buscando ataques conocidos antes de que puedan llegar a una máquina virtual recién provisionado o arrancada. También es posible aplicar **NAC**¹¹⁹ (control de acceso a la red) con capacidades para aislar las VM hasta que sus reglas y archivos de patrones sean actualizados y se haya ejecutado un escaneo.

13.1.7 Cifrado VM

Las imágenes de máquinas virtuales son vulnerables al robo o a la modificación cuando están en reposo o en marcha. La solución a este problema es cifrar las imágenes de máquinas virtuales en todo momento, pero esto plantea problemas de rendimiento. Para entornos de alta seguridad o regulados, el impacto en el rendimiento vale la pena. El cifrado debe combinarse con controles administrativos, DLP, y pistas de auditoría para evitar que una instantánea (*snapshot*) de una máquina virtual en ejecución escape, lo que daría al atacante la posibilidad de acceder a los datos incluidos en la instantánea VM.

13.1.8 Mezcla de datos

Existe la preocupación de que las diferentes clases de datos (o VM alojando diferentes clases de datos) puedan mezclarse en la misma máquina física. En términos de **PCI**¹²⁰, se denomina a esto despliegue en modo mixto. Se recomienda utilizar una combinación de VLANs, cortafuegos e **IDS/IPS**¹²¹ para asegurar el aislamiento de VM como un mecanismo para soportar las implementaciones en modo mixto. También se recomienda usar la categorización de datos y la gestión basada en políticas (por ejemplo, DLP) para evitar esto. En los entornos *Cloud*, todos los usuarios en el entorno virtual *multi-tenant* podrían compartir potencialmente el mínimo común denominador de la seguridad.

13.1.9 Destrucción de datos en VM

Cuando una VM se mueve de un servidor físico a otro, las empresas necesitan garantías de que no se deja información en el disco que pudiera ser recuperada por otro usuario o cuando el disco es desechado. La puesta a cero de la memoria/almacenamiento o el cifrado de todos los datos son soluciones a este problema. Las claves de cifrado se deben almacenar en un servidor de claves basado en políticas fuera del entorno virtual. Además, si se migra una VM mientras está en ejecución, puede estar en riesgo en sí misma durante la migración si el cifrado, o el borrado adecuado, no se usan.

13.1.10 Manipulación de imágenes de VM

Los *appliance* virtuales pre-configurados y las imágenes de máquinas pueden estar mal configurados o pueden haber sido manipulados antes de empezar a usarlos.

¹¹⁹ **NAC** - Network Access Control

¹²⁰ **PCI** - Payment Card Industry

¹²¹ **IDS** - Intrusion Detection Systems; **IPS**- Intrusion Prevention Systems

13.1.11 Migración de VM

La capacidad única de mover máquinas virtuales de un servidor físico a otro crea una complejidad para las auditorías y la monitorización de seguridad. En muchos casos, las máquinas virtuales pueden ser reubicadas en otro servidor físico (independientemente de su ubicación geográfica) sin crear una alerta o huella susceptible de ser una pista de auditoría.

13.2 Recomendaciones

- Los clientes deberían identificar qué tipos de virtualización utiliza el proveedor *Cloud* si es que usa alguno.
- Los implementadores deberían considerar un enfoque por zonas con entornos de producción independientes de los de prueba/desarrollo y datos/cargas de trabajo muy delicadas.
- Los implementadores deberían considerar el rendimiento cuando prueben e instalen herramientas de seguridad para máquinas virtuales, ya que los resultados varían ampliamente. Es importante considerar que las herramientas de seguridad de servidor y redes estén preparadas para la virtualización.
- El cliente debería evaluar, negociar y perfeccionar los acuerdos de licencias con los principales proveedores en entornos virtualizados.
- Los implementadores deberían asegurar cada sistema operativo virtualizado usando software de bastionado en cada instancia alojada o usar una máquina virtual en línea combinada con **APIs** del *hipervisor*.
- Los sistemas operativos virtualizados deberían ser reforzados mediante las medidas de seguridad incorporadas, aprovechando la tecnología de seguridad de terceros para proporcionar controles de seguridad por capas y reducir la dependencia exclusiva del proveedor de la plataforma.
- Los implementadores deberían velar por que las configuraciones seguras por defecto siguen o superan los niveles básicos aceptados por la industria.
- Los implementadores deberían cifrar las imágenes de máquinas virtuales cuando no estén en uso.
- Los implementadores deberían estudiar la eficacia y la viabilidad de la segregación de VM y la creación de zonas de seguridad por tipo de uso (por ejemplo, escritorio frente a servidor), la etapa de producción (por ejemplo, desarrollo, producción y pruebas), y la delicadeza de los datos mediante componentes de hardware físicamente separados tales como servidores, almacenamiento, etc.
- Los implementadores deberían asegurarse de que las herramientas o servicios de evaluación de vulnerabilidades de seguridad cubren las tecnologías de virtualización utilizadas.
- Los implementadores deberían considerar la implementación de soluciones de localización automática de datos y etiquetado (por ejemplo, DLP) con alcance a toda la organización para aumentar la clasificación de datos y el control entre las máquinas virtuales y entornos.
- Los implementadores deberían considerar el parchear las imágenes de máquinas virtuales en reposo o proteger las nuevas hasta que se puedan parchear.

- Los implementadores deberían entender qué controles de seguridad existen de forma externa a las VM para proteger los interfaces administrativos (basado en la web, API, etc.) expuestos a los clientes.

13.3 Requerimientos

- ✓ Los mecanismos de seguridad específicos de las VM incorporados en las APIs del *hipervisor* deben utilizarse para proporcionar una monitorización granular del tráfico que pasa por las *backplanes* de las VM, el cual es opaco a los controles tradicionales de seguridad de red.
- ✓ Los implementadores deben actualizar la política de seguridad a fin de reflejar los nuevos desafíos de seguridad generados por la virtualización.
- ✓ Los implementadores deben cifrar los datos accedidos por las máquinas virtuales utilizando servidores de claves basados en políticas que almacenan las claves separadamente de la máquina virtual y de los datos.
- ✓ Los clientes deben ser conscientes de las situaciones de *multi-tenancy* con sus VM donde las preocupaciones regulatorias pueden requerir una segregación.
- ✓ Los usuarios deben validar el pedigrí y la integridad de cualquier imagen o plantilla de VM procedente de cualquier tercero, o mejor aún, crear sus propias instancias de VM.
- ✓ Los sistemas operativos virtualizados deben incluir *firewall* (entrante/saliente), sistema de prevención de intrusiones en *host* (**HIPS**)¹²², sistema de prevención de intrusiones en red (**NIPS**)¹²³, protección de aplicaciones web, antivirus, monitorización de integridad de archivos, monitorización de logs, etc. Las contramedidas de seguridad pueden ser desplegadas a través de software en cada instancia virtual alojada o utilizando una máquina virtual en línea en combinación con las APIs del *hipervisor*.
- ✓ Los proveedores deben limpiar cualquier copia de seguridad y sistema de respaldo cuando elimine y borre las imágenes de VM.
- ✓ Los proveedores deben tener implantado un mecanismo de reporte que ofrezca pruebas del aislamiento y active alertas si hay una violación del aislamiento.

¹²² **HIPS** - *Host Intrusion Prevention System*

¹²³ **NIPS** - *Network Intrusion Prevention System*

DOMINIO 14 //

SECURITY AS A SERVICE

Cloud Computing significa uno de los cambios de mayor envergadura experimentados en el uso de las tecnologías de la información por el tejido empresarial, hasta llegar a una situación en que la disponibilidad de capacidad de cálculo como servicio representa una prometedora fuente de oportunidades de expansión y de innovación. Una de estas innovaciones es la centralización de los recursos dedicados a la seguridad. La industria de la seguridad reconoce los beneficios que aporta un marco de referencia estandarizado de seguridad tanto para los proveedores de estos servicios como para sus usuarios. Este marco de referencia, en el ámbito de un ANS de *Cloud* entre proveedor y cliente, se formaliza como un documento que describe los servicios de seguridad que se van a proporcionar, y cómo y dónde se proporcionarán dichos servicios. Al madurar y consolidarse las ofertas de servicios de seguridad basadas en marco de referencia estándar, los usuarios de los mismos han podido reconocer la conveniencia de centralizar los recursos de computación. Uno de los hitos del proceso de madurez de *Cloud* como plataforma de servicios empresariales es la adopción global de Security as a Service (SecaaS) y el reconocimiento de cómo se puede mejorar en la prestación de servicios de seguridad. La implantación a escala mundial de servicios de seguridad como una funcionalidad estándar llegará a, finalmente, eliminar la variabilidad de la seguridad en las implementaciones y las carencias de seguridad.

SecaaS se enfoca a prestar servicios de seguridad para las empresas desde el *Cloud*. Y éste es lo que le diferencia del resto de trabajos e investigaciones en seguridad en el *Cloud*. Las discusiones en este campo han estado enfocadas recurrentemente en cómo migrar hacia la *Cloud* y cómo asegurar en el *Cloud* las necesidades de confidencialidad, integridad, disponibilidad y ubicación física. SecaaS lo analiza desde otro punto de vista, enfocándose en cómo hacer seguros los sistemas y la información en el *Cloud* así como las redes corporativas tradicionales o híbridas mediante servicios *Cloud*. Estos sistemas pueden estar en el *Cloud* o ubicadas de forma más tradicional en las instalaciones del cliente. Un ejemplo de esto pueden ser los servicios antispam o anti-virus.

Introducción. Este dominio tratará de los siguientes temas:

- La ubicuidad de SecaaS en el mercado
- Aspectos a valorar al implantar SecaaS
- Ventajas del uso de SecaaS
- La variedad de servicios susceptibles de ser considerados SecaaS

Este documento se relaciona con las publicaciones previas sobre SecaaS y con los controles de la CSA Cloud Control Matrix (CCM)

14.1 La ubicuidad del SecaaS en el mercado

Los usuarios tienen sensaciones mezcladas de interés y de preocupación ante las perspectivas que ofrece el *Cloud Computing*. Despiertan interés las oportunidades que ofrece de reducción de los costes de inversión en equipamientos y de desentenderse de la administración diaria de los sistemas para enfocarse en competencias clave. Y sobre todo, la agilidad de respuesta que proporciona la provisión bajo demanda de recursos, y la facilidad para alinear con rapidez y precisión los sistemas de Información con las necesidades y estrategias de negocio. Sin embargo, los clientes están preocupados por los riesgos de seguridad que conlleva el *Cloud* y con la pérdida de control directo sobre los sistemas de seguridad sobre los que se les exigen responsabilidades. Los fabricantes han tratado de satisfacer esta necesidad de seguridad ofreciendo servicios de seguridad instalados en una plataforma en *Cloud*, pero solo han logrado causar

confusión en el mercado y complicar el proceso de selección de tecnologías, en tanto que cada servicio se ha diseñado y ofrecido de forma individual y sin transparencia sobre los controles de seguridad que en él se incorporan. Todo ello ha provocado que a la fecha, la adopción de servicios de seguridad basados en *Cloud* sea limitada. SecaaS está experimentando crecimientos exponenciales, incluso Gartner predice que al menos se triplicará su uso en diversos sectores en el año 2013.

Muchos fabricantes de seguridad están apoyándose en modelos basados en *Cloud* para prestar servicios de seguridad. Esta evolución se debe a diversas razones, como el aprovechamiento de economías de escala, o la automatización en la entrega de servicios. Los usuarios deben evaluar con mayor frecuencia la seguridad de soluciones que no se encuentran en sus oficinas. Los usuarios necesitan entender la naturaleza particular, diversa y ubicua de la oferta de servicios entregados desde *Cloud*, para que estén capacitados para evaluar los servicios ofertados y puedan valorar si dichos servicios satisfacen sus necesidades.

14.2 Aspectos a valorar al implantar SecaaS

A pesar del amplio conjunto de beneficios ofrecidos por los servicios de seguridad desde *Cloud*, tales como su escalabilidad, provisión de recursos virtualmente ilimitada o las economías de escala con costes de adquisición reducidos o nulos, hay algunos aspectos que deben ser valorados en un entorno *Cloud*. Algunos de ellos se refieren al cumplimiento legal, a *multi-tenancy*, y al *lock-in* con proveedores. Si bien se señala a estos aspectos como responsables del retraso en la migración de las soluciones de seguridad a *Cloud*, están igualmente presentes en los CPDs tradicionales.

En muchas ocasiones, las valoraciones sobre la seguridad de los entornos *Cloud* se preocupan sobre si la falta de transparencia por parte de los proveedores sobre los controles de seguridad implantados en *Cloud* se debe a que no están implantados al mismo nivel que en los Centros de Proceso de Datos tradicionales, y a si existen carencias en la verificación de los antecedentes y acreditaciones del personal que opera los entornos *Cloud*. Los proveedores de SecaaS reconocen la facilidad con la que esta duda puede plantearse y por ello, habitualmente sobreimplantan controles de seguridad en sus entornos para asegurar tanto como sea posible su seguridad. Esto habitualmente incluye verificaciones de antecedentes personales comparables a los más rígidos efectuados por las administraciones públicas, y los repiten periódicamente. La seguridad física y del personal es una de las prioridades más altas de un proveedor SecaaS.

El cumplimiento legal también se ha señalado como un aspecto a estudiar, puesto que el cumplimiento legal por un proveedor debe ser global, como global es su servicio. Los proveedores SecaaS han identificado este aspecto, y han invertido un esfuerzo considerable en demostrar el cumplimiento por su parte de estos requisitos, incluso por encima de lo estrictamente necesario, o para integrarlo en las redes de sus clientes. Los proveedores de SecaaS deben ser conocedores de las regulaciones nacionales o regionales que afectan a sus servicios y a sus usuarios, y cómo incluirlas como parte de sus servicios y de su implementación. Los proveedores SecaaS más avanzados suelen incluir servicios de mediación y asesoría legal para adelantarse a las necesidades regulatorias que requiera un sector o un territorio. Además, al aplicar SecaaS en sectores fuertemente regulados, se deberán incluir en el ANS las métricas y KPIs que definen las necesidades regulatorias establecidas para ese caso, asegurando así que se alcanzan los objetivos regulatorios necesarios.

Como en cualquier servicio *Cloud*, *multi-tenancy* puede implicar problemas de fugas de información entre las múltiples instancias virtuales. Al igual que preocupa a los usuarios, también los proveedores SecaaS están muy preocupados, en particular ante la posibilidad de que se entablen litigios o demandas por este motivo. En consecuencia, los servicios de mayor madurez aplican numerosas medidas para asegurar que los datos están convenientemente aislados, y que los

datos que se comparten se hacen anónimos de forma que se proteja su identidad y fuente. Esto se aplica por igual a los datos en los que presta servicio el proveedor SecaaS, y a los que genera en la prestación del mismo y que el proveedor custodia, tales como logs o registros de auditoría en el proveedor o en los sistemas de información del cliente.

Otro aspecto en que los procesos legales afectan al *multi-tenancy* es el aumento en el uso combinado de análisis estadístico y procesado semántico. La identificación y descripción de recursos y la jurimétrica aplicada, el análisis de precedentes jurisprudenciales para transformarlos en reglas y códigos que puedan ser usados por sistemas informáticos, pueden ser empleados proactivamente para resolver indefiniciones legales en el uso de recursos compartidos.

Cuando se recibe servicio de un proveedor SecaaS, el usuario depende del proveedor para la generación y custodia de algunos, muchos o de todos los registros de actividad, cumplimiento legal y reporte de servicio, a veces generados con estándares propietarios. Cuando se plantea la posibilidad de cambio de proveedor, el usuario debe incluir en el cambio la transferencia ordenada de estos registros, identificando y aplicando el proceso para migrar correctamente los registros existentes, incluyendo garantías para posibles usos forenses posteriores.

Es importante resaltar que, salvo en los aspectos derivados de *multi-tenancy*, estos aspectos a contemplar no son privativos de un entorno *Cloud*, y que también existen en los servicios que se prestan internamente o en modelos de externalización. Por ello, se necesita en todos los casos aplicar controles de seguridad estándar y comunes a estos escenarios. Los controles propuestos por la Matriz de Controles *Cloud* de la *Cloud Security Alliance* son un buen ejemplo de este tipo de controles

14.3 Ventajas del uso de SecaaS

Los expertos técnicos conocen bien los potenciales beneficios estratégicos de apoyarse en servicios de seguridad centralizados mediante las mejoras que observan en eficiencia de ejecución de los procesos habituales. Es el mismo caso que el uso de servicios de *Cloud* para usuarios y proveedores. Los proveedores SecaaS ofrecen múltiples beneficios en base a varios factores, incluyendo la acumulación de conocimiento, la mayor captura de información de inteligencia de seguridad y la disponibilidad permanente de equipos de profesionales de seguridad, por mencionar algunos. Las empresas que están centralizando y estandarizando activamente sus mejores prácticas en seguridad consiguen habitualmente ahorros de costes notables a medio y largo plazo, lo que deriva en mejoras de competitividad por la mejora en eficiencia conseguida. La prestación de servicios de seguridad como servicio permite a los usuarios comparar de forma estándar a los diversos proveedores, lo que ayuda a entender los servicios que reciben.

14.3.1 Ventajas Competitivas

Las empresas que se apoyan en servicios de seguridad prestados por terceros mejoran su competitividad frente a su competencia debido a que acceden antes a información valiosa para comprender los riesgos asociados a la estrategia TI que se aplica. Más aun, mediante el uso de servicios centralizados, los usuarios son capaces de impedir el uso de contenidos no deseados. Las compañías que se apoyan en terceros para asegurar el cumplimiento legal y medir los parámetros obligados por ley (tanto legales como contractuales, tanto asociados a datos como a usuarios) pueden evitar entrar en costosos litigios y demandas o en sanciones a los que su competencia también está expuesta. Una vez que se adoptan e implementan servicios holísticos de seguridad, los proveedores se benefician de la ventaja competitiva de garantizar a sus clientes que reciben los mejores servicios de seguridad. Por su parte, los usuarios de los servicios

disponen de la ventaja de incluir en su marco de cumplimiento legal a proveedores de servicios de seguridad y otros proveedores de confianza como prueba de que alcanzan los niveles de servicio que se establecen en su ANS.

14.3.2 Relación mejorada entre proveedor y usuario

Hay varios beneficios evidentes de SecaaS. La transparencia que ofrece disponer de un servicio externo de provisión de confianza permite a los usuarios entender qué servicio están recibiendo, facilitando la comparativa entre proveedores, y la adhesión de los mismos a estándares reconocidos. La disponibilidad de servicios de migración permite la migración de datos y servicios entre proveedores. Apoyándose en estos servicios, usuarios y proveedores pueden presionar a sus suministradores para mejorar a su vez sus servicios, incrementando el valor de las empresas de las que son proveedores y aumentando la seguridad de la cadena de suministro.

14.4 Variedad de servicios susceptibles de ser considerados SecaaS

SecaaS es más que un mero modelo de externalización para la gestión de la seguridad; es un componente fundamental para asegurar la resiliencia y continuidad del negocio. Respecto de la resiliencia del negocio, SecaaS ofrece varios beneficios: por la elasticidad del modelo de servicios, los usuarios solo deben pagar por los servicios que solicitan, tales como número de puestos de trabajo que se emplean, y no por un presupuesto genérico IT para sistemas de información y personal que los opere. Un proveedor especializado en seguridad ofrecerá conocimiento más experto que el habitualmente tienen las organizaciones. Finalmente, la externalización de tareas rutinarias, como la gestión de logs, permite ahorros de tiempo y dinero, lo que permite que la organización dedique más recursos a sus competencias clave.

Gartner predice que en 2013 el 60% de los ingresos de los proveedores de mensajería se originarán por controles de seguridad basados en *Cloud*, tales como *anti-malware* o *antispam*.

Se estima que los clientes estarán más interesados en recibir servicios SecaaS en estas áreas:

- Servicios de Identidad Digital y Gestión de Accesos
- *Data Loss Prevention* (DLP)
- Seguridad Web
- Seguridad del Correo Electrónico
- Evaluaciones de Seguridad
- Gestión, Detección y Prevención de Intrusos (IDS/IPS)
- Gestión de Información y Eventos de Seguridad (SIEM)
- Cifrado
- Continuidad de Negocio y Recuperación ante Desastres
- Seguridad en Red

14.4.1 Servicios de Identidad Digital y Gestión de Accesos

Identity-as-a-service (IdaaS) es un término genérico que abarca un ecosistema de servicios tales como *Policy Enforcement Points* (PEP-as-a-service), *Policy Decision Points* (PDP-as-a-service), *Policy Access Points* (PAP-as-a-service), Todos ellos son servicios de atributos de usuarios y servicios de reputación de usuarios para garantizar el acceso.

Todos estos servicios de Identidad Digital pueden ser proporcionados desde un único proveedor, varios proveedores mezclados, o de forma más habitual actualmente mediante una solución híbrida de proveedores públicos y privados, tanto IAM como *Cloud*.

Estos servicios de IDaaS deben proporcionar controles de seguridad sobre gestión de identidades, accesos y privilegios, Los servicios IDaaS incluyen las personas, procesos y sistemas que gestionan el acceso a recursos corporativos asegurando que se verifica la identidad que desea acceder, y que se asignan los accesos apropiados a dicha identidad. Los servicios aseguran que los registros de estas actividades, tales como accesos erróneos o accesos exitosos deberían ser incluidos en servicios SIEM.

14.4.2 Data Loss Prevention (DLP)

Mediante la monitorización, protección y evidencia de que se está protegiendo la información almacenada, en tránsito o en uso, tanto en el *Cloud*, como en las propias instalaciones, los servicios de *Data Loss Prevention (DLP)* ofrecen protección de la información, habitualmente mediante el uso de un agente en puestos de usuario o servidores, y aplicando políticas que detallan qué acciones se permite para determinados tipos de datos. Estas políticas se diferencian de las reglas genéricas tipo “no ftp” o “no subir a sitio web” en su grado de comprensión de la información, por ejemplo “no se pueden enviar documentos que aparentemente contengan números de tarjetas de crédito”, o “la información guardada en un USB se cifra automáticamente, y solo se puede descifrar en un puesto de usuario corporativo que tenga el cliente DLP”, o “solo los clientes con DLP pueden abrir ficheros de este servidor”. En *Cloud*, el servicio DLP puede ofrecerse como parte del diseño, de forma que se puedan crear servidores con el cliente DLP instalado por defecto y aplicando por defecto un conjunto de reglas previamente definidas. Además, DLP puede apoyar la necesidad de uso de servicios IDaaS que contengan perfiles de acceso. La capacidad de aplicar un servicio para monitorizar y controlar los flujos de datos desde la organización a los distintos servicios en *Cloud* puede usarse como un control preventivo ante escenarios de exportación de datos con regulación específica a otros países y las sanciones que de ello se deriven, como en el caso de datos de carácter personal. Esta oferta DLP es un control preventivo tecnológico.

14.4.3 Seguridad Web

Se refiere como Seguridad Web a la capacidad de ofrecer protección en tiempo real a las conexiones web realizadas contra un servidor, empleando software o un *appliance* específico, bien local bien en *Cloud*, al que se redirigen las conexiones. Esta funcionalidad añade una capa de protección adicional a las existentes para prevenir la inyección de *malware* en redes corporativas a través de la navegación. Para ello, estos elementos aplican reglas definidas, que permiten determinados tipos de tráfico y otros no, o que definen los periodos horarios en los que se permiten. La exigencia de autorización, combinada con una gestión de usuarios para ello, proporciona un nivel extra de granularidad en estos accesos. La Seguridad Web es un control reactivo, de detección y de protección.

14.4.4 Seguridad del Correo Electrónico

La Seguridad del Correo Electrónico debe proporcionar control sobre el correo entrante y el saliente, protegiendo a la organización del *phishing*, adjuntos con *malware*, y ejecutando políticas corporativas, del tipo de “uso aceptable” o “prevención de *spam*”, así como proporcionando capacidades adicionales para la continuidad de negocio. Además, esta

solución debería permitir el cifrado automático y por política del correo electrónico y la integración de soluciones de correo de múltiples fabricantes. La inclusión de firma digital en el correo para facilitar la identificación del correo y su no repudio suelen también estar incluidos en estas soluciones. La Seguridad del Correo Electrónico es un control reactivo, de detección y de protección.

14.4.5 Evaluaciones de Seguridad

Por Evaluaciones de Seguridad se entiende la realización de auditorías de los servicios *Cloud* o de las propias infraestructuras, ya sea por el propio usuario o una tercera parte, apoyándose en soluciones proporcionadas desde *Cloud* que aplican estándares de la industria. Tradicionalmente, las evaluaciones de seguridad para infraestructura, aplicaciones o las auditorías de cumplimiento legal están bien definidas y apoyadas en estándares NIST, ISO o CIS¹²⁴. Para ello, existen diversas herramientas con madurez suficiente, algunas de las cuales se han implantado como SecaaS. En este modelo, los usuarios se suscriben al uso de las herramientas concretas, y obtienen los beneficios esperables de cualquier solución *Cloud*: elasticidad, tiempo de puesta en marcha muy reducido, escasa necesidad de administración y pago por uso con escasas necesidades financieras para su arranque.

Aunque no están incluidas en el foco de esta guía, aparecen algunas dificultades adicionales cuando estas herramientas se usan para auditar al propio entorno *Cloud*. Varias organizaciones, CSA incluida, están trabajando en la preparación de guías para ayudar a que las organizaciones entiendan estas dificultades adicionales:

- Configuración de la herramienta adaptada al entorno virtual en que se ejecuta. Más evidente en herramientas de auditoría en entorno IaaS
- Necesidad de soporte de la herramienta en los *marcos de referencia* web habituales. Más evidente en PaaS.
- Controles de cumplimiento legal, tanto en IaaS, PaaS y SaaS
- Necesidad de herramientas automatizadas de notificación de incidentes e intrusiones, para el mantenimiento de la integridad de la cadena de suministro en *Cloud*
- Necesidad de cuestionarios estandarizados, para todos los entornos, que permitan afrontar
 - ¿Qué se debería probar en un entorno *Cloud*?
 - ¿Cómo se asegura el aislamiento de datos en entornos de *multi-tenancy*?
 - ¿Qué información debería contener un informe tipo e vulnerabilidades de la infraestructura?
 - ¿Es viable emplear los resultados de auditorías que facilite el propio proveedor de *Cloud*?

14.4.6 Gestión, Detección y Prevención de Intrusos (IDS/IPS)

Los Sistemas de Detección/Prevención de Intrusos vigilan patrones de actividad, empleando modelos basados en reglas, en heurísticos o en patrones para detectar anomalías en las actividades de los Sistemas de Información que pudieran derivar en riesgos para la empresa. Los IDS/IPS de red han pasado a ser ampliamente usados en la primera década del

¹²⁴ CIS-Center for Internet Security

siglo XXI por la visión granular de lo que estaba pasando en la red que ofrecen. Los IDS/IPS monitorizan el tráfico de red, comparando las secuencias de tráfico que detectan con el tráfico habitual, mediante el uso de reglas o análisis estadístico. Los IDS normalmente se configuran en modo pasivo, para monitorizar (pasivamente) determinados segmentos de red delicados de la red, mientras que los IPS se configuran en modo activo para que puedan (activamente) defender las redes que monitorizan. En una infraestructura tradicional, estas redes podían ser Redes DesMilitarizadas (o DMZ)¹²⁵, creadas por routers o cortafuegos y que albergan servidores web, o conexiones a servidores internos de bases de datos. En *Cloud*, los IDS se suelen configurar en los servidores virtuales, o en las comunicaciones entre hipervisores, donde los ataques pueden afectar a varios clientes y lograr crear un mayor caos. Los IDS son controles de detección mientras que los IPS son de detección, protección y reactivos.

14.4.7 Gestión de Información y Eventos de Seguridad (SIEM)

Los Gestores de Información y Eventos de Seguridad (SIEM) centralizan (ya sea en modo *pull* o en modo *push*) logs y otros registros de eventos, generados por redes, aplicaciones y sistemas reales y virtuales. La información recogida es después correlada y analizada para ofrecer la capacidad de generar informes en tiempo real, emitir alertas sobre información o eventos que pudieran requerir intervención humana u otro tipo de respuestas. La recogida y archivo de logs se realiza típicamente de forma que se pueda prevenir alteraciones de los datos, de forma que los logs recogidos puedan emplearse como evidencia en investigaciones o generación de informes a largo plazo. SIEM es un control de detección, pero puede configurarse para ser de prevención o de reacción

14.4.8 Cifrado

El cifrado es el proceso de ofuscar o recodificar datos utilizando algoritmos criptográficos, para producir datos cifrados (también llamado texto cifrado). Sólo el receptor (persona o sistema) para quien se ha realizado este proceso y que está en posesión de la clave correcta puede decodificar (descifrar) el texto cifrado. Los sistemas de cifrado por ofuscación típicamente consisten en uno o más algoritmos computacionalmente complejos y difíciles de rehacer en orden inverso, una o más claves, y los sistemas, procesos y procedimientos necesarios para gestionar el cifrado, el descifrado, y el ciclo de vida de las claves. Así, cada elemento de este proceso es ineficaz si los demás son débiles. Por ejemplo, el texto cifrado con el mejor algoritmo puede ser fácilmente descifrado si se puede acceder a las claves con facilidad por no haberse protegido suficientemente este elemento.

Para los algoritmos criptográficos unidireccionales, su aplicación crea en cambio un resumen o *hash* del texto inicial. Entre estos algoritmos se incluyen los algoritmos de *hashing*, de firma digital, de generación y renovación de certificados digitales y de intercambio de claves. Estos sistemas, típicamente, constan de uno o más algoritmos que son fáciles de computar, pero muy difíciles de falsificar, así como de nuevo los procesos y procedimientos necesarios para su gestión. El cifrado, cuando se hace desde un proveedor SecaaS se clasifica como un control de protección y de detección.

14.4.9 Continuidad de Negocio y Recuperación ante Desastres

La Continuidad de Negocio y la Recuperación ante Desastres son los procedimientos diseñados e implantados para asegurar la resiliencia de las operaciones de la organización ante posibles interrupciones de servicio. Proporcionan

¹²⁵ DMZ-De-Militarized Zone

alternativas flexibles y confiables que usar como respaldo para los servicios que sean precisos en una interrupción de servicio, ya sea natural o provocada por el hombre. Por ejemplo, si ocurre un desastre en una ubicación, los servicios pueden ser replicados en sistemas de información de otras ubicaciones. Este control es reactivo, de protección y de detección.

14.4.10 Seguridad en Red

Por Seguridad en Red se entienden los servicios de seguridad que limitan o permiten accesos y que reparten, monitorizan, generan logs y proteger los recursos que emplean los servicios TI.

Desde un punto de vista de arquitectura del servicio, la Seguridad en Red proporcionan servicios que proporcionan controles de seguridad al total de la red, o a redes particulares de cada recurso específico. En entornos de *Cloud* pura o híbrida, la seguridad en red probablemente sea suministrada conjuntamente por dispositivos reales y virtuales. Es clave la integración de este servicio con el hipervisor para garantizar visibilidad completa de todo el tráfico en la red, ya sea física o virtual. La Seguridad en Red incluye controles de detección, prevención y reactivos.

14.5 Autorizaciones

- Los usuarios de servicios pueden emplear técnicas de reconocimiento de patrones para la actividad de usuarios.
- Los usuarios de servicios pueden emplear valoraciones legales de las métricas de seguridad para la gestión de las expectativas recogidas en el ANS.
- Los usuarios de servicios pueden emplear canales confiables para realizar test de intrusión.

14.6 Recomendaciones

- Los usuarios del servicio deben asegurarse de la existencia de canales de comunicación seguros entre el proveedor y el usuario de los servicios.
- Los proveedores de servicio deberían facilitar notificaciones automatizadas, seguras y continuas a toda la cadena de suministro del servicio, en base a su necesidad de conocer.
- Los proveedores de servicio deberían proporcionar registros de actividad confiables de las operaciones internas de su servicio, a efectos de facilitar la verificación del ANS.
- Los usuarios debería solicitar la colaboración de terceras partes, tanto en servicios de auditoría del proveedor como de medición del ANS.
- Todas las partes deberían emplear Monitorización Continua en todas las interfaces de servicio a través de, por ejemplo, SCAP (NIST), CYBEX (ITU-T), o RID & IODEF (IETF).

14.7 Requisitos

14.7.1 Requisitos de los Servicios de Identidad Digital y Gestión de Accesos

- ✓ Los proveedores de IDaaS deben proporcionar a sus clientes de servicios *Cloud* mecanismos de aprovisionamiento y desaprovisionamiento de usuarios, tanto en el entorno *Cloud* como en el interno, tanto para aplicaciones como para otros recursos.
- ✓ Los proveedores de IDaaS deben proporcionar a sus clientes de servicios *Cloud* servicios de autenticación (soportando múltiples métodos y factores de autenticación).
- ✓ Los proveedores de IDaaS debe proporcionar a sus clientes de servicios *Cloud* servicios de gestión del ciclo de vida de las identidades.
- ✓ Los proveedores de IDaaS deben proporcionar a sus clientes de servicios *Cloud* servicios de directorio.
- ✓ Los proveedores de IDaaS deben proporcionar a sus clientes de servicios *Cloud* servicios de sincronización entre directorios, cubriendo incluso esquemas multilaterales.
- ✓ Los proveedores de IDaaS deben proporcionar a sus clientes de servicios *Cloud* servicios de federación de identidades y SSO.
- ✓ Los proveedores de IDaaS deben proporcionar a sus clientes de servicios *Cloud* servicios de SSO Web, entendido como gestión de sesiones y control de acceso granular a través de servicios web, no como federación.
- ✓ Los proveedores de IDaaS deben proporcionar a sus clientes de servicios *Cloud* monitorización de sesiones con privilegios de acceso: Administradores, etc.
- ✓ Los proveedores de IDaaS deben proporcionar a sus clientes de servicios *Cloud* la posibilidad de hacer una gestión de acceso granular.
- ✓ Los proveedores de IDaaS deben proporcionar a sus clientes de servicios *Cloud* servicios de sellado digital u otros métodos que garanticen la validez de los registros de auditoría generados, incluyendo también opciones para activar características de no repudio.
- ✓ Los proveedores de IDaaS deben proporcionar a sus clientes de servicios *Cloud* servicios de gestión de políticas de acceso, incluyendo gestión de roles, de autorización y de cumplimiento legal.
- ✓ Los proveedores de IDaaS deben proporcionar a sus clientes de servicios *Cloud* servicios de autorización de acceso, tanto de usuarios como de aplicaciones.
- ✓ Los proveedores de IDaaS deben proporcionar a sus clientes de servicios *Cloud* servicios de gestión de tokens de autenticación: gestión de los mismos, provisión.
- ✓ Los proveedores de IDaaS deben proporcionar a sus clientes de servicios *Cloud* servicios de gestión de perfiles de usuario y concesión de autorización, tanto de usuarios como de aplicaciones.

- ✓ Los proveedores de IDaaS deben proporcionar a sus clientes de servicios *Cloud* soporte para la monitorización y generación de informes de cumplimiento legal y de políticas del cliente.
- ✓ Los proveedores de IDaaS deben proporcionar a sus clientes de servicios *Cloud* servicios de aprovisionamiento federado de aplicaciones *Cloud*.
- ✓ Los proveedores de IDaaS deben proporcionar a sus clientes de servicios *Cloud* accesos y contraseñas de usuario privilegiado, incluyendo accesos de administración, accesos compartidos, accesos al sistema y accesos a las aplicaciones.
- ✓ Los proveedores de IDaaS deben proporcionar a sus clientes de servicios *Cloud* servicios RBAC
- ✓ Los proveedores de IDaaS deben proporcionar a sus clientes de servicios *Cloud* soporte para la integración con DLP.
- ✓ Los proveedores de IDaaS deben proporcionar a sus clientes de servicios *Cloud* soporte para la auditoría de las actividades con granularidad suficiente, incluyendo la monitorización de usuarios individuales.
- ✓ Los proveedores de IDaaS deben proporcionar a sus clientes de servicios *Cloud* la segregación de responsabilidades basadas en la concesión de permisos adecuadas a las distintas identidades digitales implicadas.
- ✓ Los proveedores de IDaaS deben proporcionar a sus clientes de servicios *Cloud* la generación de informes orientados al cumplimiento legal.
- ✓ Los proveedores de IDaaS deben proporcionar a sus clientes de servicios *Cloud* la gestión de políticas centralizadas.
- ✓ Los proveedores de IDaaS deben proporcionar a sus clientes de servicios *Cloud* interfaces de gestión útiles.
- ✓ Los proveedores de IaaS deben proporcionar a sus clientes de servicios *Cloud* un control de acceso y auditoría unificados.
- ✓ Los proveedores de IaaS deben proporcionar a sus clientes de servicios *Cloud* interoperabilidad entre diversos proveedores, incluso proveedores heterogéneos
- ✓ Los proveedores de IaaS deben proporcionar a sus clientes de servicios *Cloud* escalabilidad

14.7.2 Requisitos de DLP SecaaS

- ✓ Los proveedores de DLP deben proporcionar a sus clientes de servicios *Cloud* etiquetado y clasificación de datos.
- ✓ Los proveedores de DLP deben proporcionar a sus clientes de servicios *Cloud* identificación de datos delicados.
- ✓ Los proveedores de DLP deben proporcionar a sus clientes de servicios *Cloud* políticas predefinidas adaptadas a las principales regulaciones legales.
- ✓ Los proveedores de DLP deben proporcionar a sus clientes de servicios *Cloud* heurísticos de detección de contexto.

- ✓ Los proveedores de DLP deben proporcionar a sus clientes de servicios *Cloud* servicios de “*structured data matching*”, para los datos almacenados.
- ✓ Los proveedores de DLP deben proporcionar a sus clientes de servicios *Cloud* detección de expresiones regulares SQL.
- ✓ Los proveedores de DLP deben proporcionar a sus clientes de servicios *Cloud* servicios de detección de patrones de tráfico para datos en tránsito.
- ✓ Los proveedores de DLP deben proporcionar a sus clientes de servicios *Cloud* servicios de aviso al usuario en tiempo real.
- ✓ Los proveedores de DLP deben proporcionar a sus clientes de servicios *Cloud* asignación de nivel de seguridad de acceso.
- ✓ Los proveedores de DLP deben proporcionar a sus clientes de servicios *Cloud* búsqueda personalizada de atributos.
- ✓ Los proveedores de DLP deben proporcionar a sus clientes de servicios *Cloud* servicios de respuesta automatizada ante incidentes.
- ✓ Los proveedores de DLP deben proporcionar a sus clientes de servicios *Cloud* la firma de datos.
- ✓ Los proveedores de DLP deben proporcionar a sus clientes de servicios *Cloud* protección criptográfica de los datos y control de acceso a los mismos.
- ✓ Los proveedores de DLP deben proporcionar a sus clientes de servicios *Cloud* un lenguaje de descripción de políticas adecuado para su uso por los Sistemas de Información

14.7.3 Requisitos de Servicios Web SecaaS

- ✓ Los proveedores de Servicios Web SecaaS deben proporcionar a sus clientes de servicios *Cloud* monitorización y filtrado de tráfico web.
- ✓ Los proveedores de Servicios Web SecaaS deben proporcionar a sus clientes de servicios *Cloud* servicios de análisis y bloqueo de *malware*, *spyware* y arranque desde red.
- ✓ Los proveedores de Servicios Web SecaaS deben proporcionar a sus clientes de servicios *Cloud* bloqueo de sitios identificados como *phishers*.
- ✓ Los proveedores de Servicios Web SecaaS deben proporcionar a sus clientes de servicios *Cloud* servicios de verificación de servicios y tráfico de mensajería instantánea.
- ✓ Los proveedores de Servicios Web SecaaS deben proporcionar a sus clientes de servicios *Cloud* servicios de seguridad de correo electrónico.
- ✓ Los proveedores de Servicios Web SecaaS deben proporcionar a sus clientes de servicios *Cloud* servicios de gestión de ancho de banda, y control de volumen de tráfico en red.

- ✓ Los proveedores de Servicios Web SecaaS deben proporcionar a sus clientes de servicios *Cloud* servicios DLP.
- ✓ Los proveedores de Servicios Web SecaaS deben proporcionar a sus clientes de servicios *Cloud* servicios de prevención del fraude.
- ✓ Los proveedores de Servicios Web SecaaS deben proporcionar a sus clientes de servicios *Cloud* control de acceso vía Web.
- ✓ Los proveedores de Servicios Web SecaaS deben proporcionar a sus clientes de servicios *Cloud* servicios de *backup*.
- ✓ Los proveedores de Servicios Web SecaaS deben proporcionar a sus clientes de servicios *Cloud* servicios de gestión de SSL, permitiendo su descifrado y monitorización.
- ✓ Los proveedores de Servicios Web SecaaS deben proporcionar a sus clientes de servicios *Cloud* políticas de usos aceptables.
- ✓ Los proveedores de Servicios Web SecaaS deben proporcionar a sus clientes de servicios *Cloud* servicios de gestión de vulnerabilidades.
- ✓ Los proveedores de Servicios Web SecaaS deben proporcionar a sus clientes de servicios *Cloud* servicios de informes de inteligencia de uso de Web.

14.7.4 Requisitos de Correo Electrónico SecaaS

- ✓ Los proveedores de Correo Electrónico SecaaS deben proporcionar a sus clientes de servicios *Cloud* servicios de filtrado confiables para el bloqueo de *spam* y de *phishing*
- ✓ Los proveedores de Correo Electrónico SecaaS deben proporcionar a sus clientes de servicios *Cloud* protección efectiva contra virus y *spyware* antes de que estos contenidos superen los perímetros de seguridad.
- ✓ Los proveedores de Correo Electrónico SecaaS deben proporcionar a sus clientes de servicios *Cloud* políticas flexibles de uso del servicio, para poder definir tratamientos particulares para flujos de correo específicos así como políticas de cifrado de correo.
- ✓ Los proveedores de Correo Electrónico SecaaS deben proporcionar a sus clientes de servicios *Cloud* informes de actividad completos, interactivos y en tiempo real.
- ✓ Los proveedores de Correo Electrónico SecaaS deben proporcionar a sus clientes de servicios *Cloud* inspección en profundidad de contenidos, para la completa aplicación de las políticas aprobadas.
- ✓ Los proveedores de Correo Electrónico SecaaS deben proporcionar a sus clientes de servicios *Cloud* capacidad para cifrar todos o parte de los correos, de acuerdo con las políticas que se definan.
- ✓ Los proveedores de Correo Electrónico SecaaS deben proporcionar a sus clientes de servicios *Cloud* capacidad de integración con servidores de correo de distintos fabricantes.

14.7.5 Requisitos de Evaluaciones de Seguridad SecaaS

- ✓ Los proveedores de Evaluaciones de Seguridad SecaaS deben proporcionar a sus clientes de servicios *Cloud* de forma detallada los procesos de gobierno y las métricas que se aplican en ellos. Los usuarios deberán haber definido y documentado su proceso de toma de decisiones y aplicación de políticas.
- ✓ Los proveedores de Evaluaciones de Seguridad SecaaS deben proporcionar a sus clientes de servicios *Cloud* un servicio automatizado de notificación de incidentes de seguridad a toda la cadena de suministros
- ✓ Los proveedores de Evaluaciones de Seguridad SecaaS deben proporcionar a sus clientes de servicios *Cloud* una gestión del riesgo adecuada. Los usuarios deberían definir y documentar el proceso por el que se aseguran de que los comportamientos y procesos de negocio más importantes quedan dentro de los límites de tolerancia de riesgo asociados a las políticas y decisiones corporativas.
- ✓ Los proveedores de Evaluaciones de Seguridad SecaaS deben proporcionar a sus clientes de servicios *Cloud* detalles de su cumplimiento legal. Los usuarios deberían definir y documentar sus procesos de aseguramiento del cumplimiento legal.
- ✓ Los proveedores de Evaluaciones de Seguridad SecaaS deben proporcionar a sus clientes de servicios *Cloud* políticas propias derivadas de decisiones, procedimientos o requisitos internos, y con leyes, regulaciones, estándares y acuerdos externos.
- ✓ Los proveedores de Evaluaciones de Seguridad SecaaS deben proporcionar a sus clientes de servicios *Cloud* auditorías de cumplimiento técnicas de sus propias plataformas, incluyendo la auditoría automatizada de dispositivos, sistemas operativos, gestores de bases de datos y aplicaciones.
- ✓ Los proveedores de Evaluaciones de Seguridad SecaaS deben proporcionar a sus clientes de servicios *Cloud* servicios de evaluación automatizada de seguridad de aplicaciones particulares.
- ✓ Los proveedores de Evaluaciones de Seguridad SecaaS deben proporcionar a sus clientes de servicios *Cloud* servicios de evaluación de vulnerabilidades, identificando vulnerabilidades conocidas y errores de configuración en dispositivos, sistemas operativos, gestores de bases de datos y aplicaciones.
- ✓ Los proveedores de Evaluaciones de Seguridad SecaaS deben proporcionar a sus clientes de servicios *Cloud* servicios de test de intrusión, que incluyan el aprovechamiento de las vulnerabilidades y de los errores de configuración para lograr acceder a entornos, equipos y otros elementos. Este servicio puede ser no automatizado y requerir la intervención de expertos.
- ✓ Los proveedores de Evaluaciones de Seguridad SecaaS deben proporcionar a sus clientes de servicios *Cloud* un servicio de valoración de la seguridad del cliente.

14.7.6 Requisitos de IDS/IPS SecaaS

- ✓ Los proveedores de IDS/IPS SecaaS deben proporcionar a sus clientes de servicios *Cloud* la identificación de intentos de intrusión y de violaciones de las políticas establecidas.

- ✓ Los proveedores de IDS/IPS SecaaS deben proporcionar a sus clientes de servicios *Cloud* la capacidad de respuesta ante incidentes, ya sea manual o automática.
- ✓ Los proveedores de IDS/IPS SecaaS deben proporcionar a sus clientes de servicios *Cloud* la gestión de los tráficos de reparto de carga y operaciones de virtualización generados por un hipervisor.
- ✓ Los proveedores de IDS/IPS SecaaS deben proporcionar a sus clientes de servicios *Cloud* la inspección de paquetes en profundidad, utilizando una o varias de estas técnicas: Estadística, de comportamiento, heurística, basada en firmas.
- ✓ Los proveedores de IDS/IPS SecaaS deben proporcionar a sus clientes de servicios *Cloud* la monitorización de las operaciones de llamada al sistema operativo.
- ✓ Los proveedores de IDS/IPS SecaaS deben proporcionar a sus clientes de servicios *Cloud* la inspección de logs de sistema y aplicaciones.
- ✓ Los proveedores de IDS/IPS SecaaS deben proporcionar a sus clientes de servicios *Cloud* la monitorización de la integridad de los sistemas operativos, incluyendo integridad de ficheros, el registro, puertos, procesos, software instalado y otros
- ✓ Los proveedores de IDS/IPS SecaaS deben proporcionar a sus clientes de servicios *Cloud* la monitorización de la integridad de hipervisores
- ✓ Los proveedores de IDS/IPS SecaaS deben proporcionar a sus clientes de servicios *Cloud* la monitorización de los repositorios de máquinas virtuales de un sistemas de virtualización

14.7.7 Requisitos de SIEM SecaaS

- ✓ Los proveedores de SIEM SecaaS deben proporcionar a sus clientes de servicios *Cloud* la recogida en tiempo real de logs y eventos, duplicación de esta información, su normalización, análisis acumulado y visualización.
- ✓ Los proveedores de SIEM SecaaS deben proporcionar a sus clientes de servicios *Cloud* apoyo en procesos forenses.
- ✓ Los proveedores de SIEM SecaaS deben proporcionar a sus clientes de servicios *Cloud* informes de cumplimiento legal y de ANS
- ✓ Los proveedores de SIEM SecaaS deben proporcionar a sus clientes de servicios *Cloud* soporte a la generación de informes detallados
- ✓ Los proveedores de SIEM SecaaS deben proporcionar a sus clientes de servicios *Cloud* detección anomalías, para más servicios que el de correo electrónico.
- ✓ Los proveedores de SIEM SecaaS deben proporcionar a sus clientes de servicios *Cloud* soporte a la generación de informes detallados
- ✓ Los proveedores de SIEM SecaaS deben proporcionar a sus clientes de servicios *Cloud* flexibilidad en los tiempos de los periodos de conservación de logs, y flexibilidad en las políticas de gestión de estos periodos.

14.7.8 Requisitos de cifrado SecaaS

- ✓ Los proveedores de cifrado SecaaS deben proporcionar a sus clientes de servicios *Cloud* protección de los datos en tránsito
- ✓ Los proveedores de cifrado SecaaS deben proporcionar a sus clientes de servicios *Cloud* protección de los datos almacenados
- ✓ Los proveedores de cifrado SecaaS deben proporcionar a sus clientes de servicios *Cloud* servicios de gestión de claves y política de uso de las mismas
- ✓ Los proveedores de cifrado SecaaS deben proporcionar a sus clientes de servicios *Cloud* protección de los datos almacenados en cachés u otros repositorios intermedios

14.7.9 Requisitos de Continuidad de Negocio y Recuperación ante Desastres SecaaS

- ✓ La Continuidad de Negocio y Recuperación ante Desastres SecaaS deben proporcionar a sus clientes de servicios *Cloud* una infraestructura flexible.
- ✓ Los proveedores de Continuidad de Negocio y Recuperación ante Desastres SecaaS deben proporcionar a sus clientes de servicios *Cloud backup* seguro.
- ✓ Los proveedores de Continuidad de Negocio y Recuperación ante Desastres SecaaS deben proporcionar a sus clientes de servicios *Cloud* monitorización de los sistemas.
- ✓ Los proveedores de Continuidad de Negocio y Recuperación ante Desastres SecaaS deben proporcionar a sus clientes de servicios *Cloud* servicios de conectividad con y hacia terceros.
- ✓ Los proveedores de Continuidad de Negocio y Recuperación ante Desastres SecaaS deben proporcionar a sus clientes de servicios *Cloud* la replicación de componentes de la infraestructura.
- ✓ Los proveedores de Continuidad de Negocio y Recuperación ante Desastres SecaaS deben proporcionar a sus clientes de servicios *Cloud* la replicación de datos de sistemas clave o críticos.
- ✓ Los proveedores de Continuidad de Negocio y Recuperación ante Desastres SecaaS deben proporcionar a sus clientes de servicios *Cloud* la recuperación de datos y/o de aplicaciones.
- ✓ Los proveedores de Continuidad de Negocio y Recuperación ante Desastres SecaaS deben proporcionar a sus clientes de servicios *Cloud* ubicaciones e instalaciones alternativas para la operación de Sistemas.
- ✓ Los proveedores de Continuidad de Negocio y Recuperación ante Desastres SecaaS deben proporcionar a sus clientes de servicios *Cloud* procesos y operaciones de recuperación probados y medidos para asegurar la resiliencia de estos procesos.
- ✓ Los proveedores de Continuidad de Negocio y Recuperación ante Desastres SecaaS deben proporcionar a sus clientes de servicios *Cloud* centros de proceso e infraestructuras distribuidos geográficamente.

- ✓ Los proveedores de Continuidad de Negocio y Recuperación ante Desastres SecaaS deben proporcionar a sus clientes de servicios *Cloud* la capacidad de vigilancia de sus propias redes.

14.7.10 Requisitos de Seguridad en Red SecaaS

- ✓ Los proveedores de Seguridad en Red SecaaS deben proporcionar a sus clientes de servicios *Cloud* detalles de las amenazas a sus datos.
- ✓ Los proveedores de Seguridad en Red SecaaS deben proporcionar a sus clientes de servicios *Cloud* detalles de las amenazas a los controles de acceso a sus datos.
- ✓ Los proveedores de Seguridad en Red SecaaS deben proporcionar a sus clientes de servicios *Cloud* controles de acceso y autenticación.
- ✓ Los proveedores de Seguridad en Red SecaaS deben proporcionar a sus clientes de servicios *Cloud* cortafuegos y otros dispositivos de conexión entre redes con seguridad: cortafuegos, WAF, SOA/API.
- ✓ Los proveedores de Seguridad en Red SecaaS deben proporcionar a sus clientes de servicios *Cloud* productos de seguridad: IDS/IPS, cortafuegos de aplicación, Monitorización de Integridad, DLP, Antivirus, antispam.
- ✓ Los proveedores de Seguridad en Red SecaaS deben proporcionar a sus clientes de servicios *Cloud* monitorización de seguridad y respuesta a incidentes.
- ✓ Los proveedores de Seguridad en Red SecaaS deben proporcionar a sus clientes de servicios *Cloud* protección o mitigación ante ataques de Denegación de Servicio.
- ✓ Los proveedores de Seguridad en Red SecaaS deben proporcionar a sus clientes de servicios *Cloud* servicios de base seguros: DNSSEC, NTP, OAuth, SNMP, segmentación de red, la propia seguridad.
- ✓ Los proveedores de Seguridad en Red SecaaS deben proporcionar a sus clientes de servicios *Cloud* monitorización de tráfico y de flujos de tráfico específicos.
- ✓ Los proveedores de Seguridad en Red SecaaS deben proporcionar a sus clientes de servicios *Cloud* integración con el hipervisor.

REFERENCIAS

[1] Security and Economic Benefits of Standardization for Security as a Service. September 2011 Proceedings. United Nations ITU-T.

[2] Gartner. Gartner Says Security Delivered as a Cloud-Based Service Will More Than Triple in Many Segments by 2013. July 15, 2008. <http://www.gartner.com/it/page.jsp?id=722307>

[3] Cloud Security Alliance. Defined Categories of Service 2011. https://cloudsecurityalliance.org/wp-content/uploads/2011/09/SecaaS_V1_0.pdf

ANEXO A //

GLOSARIO EMPLEADO

Termino Inglés	Término Español
Analytics	análisis estadístico
anonymized	hacer anónimos
API	Application Program Interface
Asset	Activo
Attached	Adjunto, Anexo
Availability	Disponibilidad
Billing	Facturación
Broker	Intermediario
Brokerage	Intermediación
Browser	Navegador
Business Intelligence	Inteligencia de Negocio
Claim	Petición
Cloud	Nube
Cloud Bursting	Proliferación de Clouds
Cloud computing	Cloud computing
Cloud deployment	Casos de Uso de Cloud
commodity	funcionalidad estándar
Community Cloud	Cloud comunitaria
Compliance	Cumplimiento Legal
Concerns	Aspectos a valorar
Confidentiality	Confidencialidad
Consumer	usuario
Content Aware Encryption	Cifrado en función del contenido
Content Delivery Network	CDN Red de distribución de contenidos
Content Discovery	Localización de Contenidos Sensibles
DaaS	DaaS
Database as a Service	
DAM	Monitorización de Actividad de Base de Datos
Database Activity Monitoring	
Data Anonymization	Disociación de datos
Data Center	CPD
Data Center Operations	Actividades del CPD
Data Comingling	mezcla de datos
Data Flow	Flujo de datos
data leakage	fugas de información
Data Security Lifecycle	Ciclo de vida de la seguridad de los datos
Defense in depth	Defensa en profundidad
DEMARC	DEMARC, Derivación de “demarcation point”
de-parameterization	eliminación de perímetros
de-provisioning	Desaprovisionamiento
DLP	DLP
Data Loss Prevention	Data Loss Prevention
DMTF	Distributed Management Task Force
Domain	Dominio
DRM	DRM
Digital Rights Management	

Termino Inglés	Término Español
EDRM Enterprise Digital Rights Management	EDRM
Encryption	Cifrado
Enforcement	Aplicación / imposición
Entitlement	Concesión de autorización asignación de derechos
Fail-over	Tolerancia a Fallos
Format Preserving encryption	Cifrado con conservación de formato
Framework	Framework Marco de Referencia
Governance	Gobierno
Guidance	Guía
Hardening	bastionado
home-based cloud	cloud de particulares
Hosting	Alojamiento
Hybrid Cloud	Cloud Híbrida
hypervisor	Hipervisor
laaS Infrastructure as a Service	laaS
IDaaS Identity-as-a-service	IDaaS
Implementers	Implementadores, Usuarios
In-house	interno
Instant-on Gaps	vulnerabilidades por parada prolongada, gaps de arranque,
Integrity	Integridad
Interoperability	Interoperabilidad
Jurimetrics	Jurimétrica
Key, Keys	Clave, Claves
<i>layered security</i>	seguridad en capas
Location	Ubicación
lock-in locked-in	lock-in locked-in
Log	Log Registro
methods of securing data	métodos para proteger los datos
Movement	Migración (en el contexto de “hacia la nube”)
Movement	Movimiento (En el contexto de “datos que van y/o vienen desde una ubicación local hacia la nube”)
Object Storage	almacenamiento de objetos
OCCI	Open Cloud Computing Interface
Overview	Introducción
OVF	Open Virtualization format
Outsourcing	externalización
passphrase	Contraseña
Pentesting	Test de Intrusión
PII Personally Identifiable Information	datos de carácter personal.
Plain text	Texto en claro
PoD	Point of delivery
Police-driven	Guiada por políticas
Portability	Portabilidad
Private Cloud Provider	Proveedor de Cloud Privada

Termino Inglés	Término Español
Processing	Capacidad de Procesado
Provisioning	Aprovisionar
Public Cloud Provider	Proveedor de Cloud Pública
Rack, racking	Rack Enracar
Raw (raw storage)	Puro (almacenamiento puro)
RBAC Role-Based Access Control	Acceso basado en roles
Responder	Equipo de Respuesta
Risk	Riesgo
SAML	Security Assertion Markup Language
SAMM Software Assurance Maturity Model	SAMM
SAPM Shared Account Password Management	SAPM
SDLC Software Development Life Cycle	Software Development Life Cycle
SecaaS Security as a Service	SecaaS
SecaaS Security-as-a-Service	SecaaS
security voids	carencias de seguridad
Sensitive data	Datos delicados Datos sensibles
service delivery	entrega de servicios
Service level	Nivel de Servicio
Single SignOn	SSO
SLA Service Level Agreement	ANS Acuerdo de Nivel de Servicio
Snapshot	Captura de pantalla Snapshot
SSE-CMM Systems Security Engineering Capability Maturity Model	SSE-CMM
structured data matching	structured data matching
Tester	Examinador
Thin-client	Clientes ligeros
Throttle	Regulación de acceso
Asses	Valorar
Evaluate	Evaluar
Tokenization	Uso de Tokens
Trade-off	Equilibrio
Trust	Confianza
UMA User Managed Access	UMA
Vendors	fabricantes
Virtual Private Storage VPS	Almacenamiento privado virtual
VM Sprawl	Proliferación de VM
VMDC	Virtual Multi-tenant Data Center
Volumen Storage	Almacenamiento de volúmenes
WS-Security	Web Services Security