# IX Foro de Seguridad RedIRIS

## Seguridad en el Cloud Computing

### Aspectos legales del Cloud computing: especial referencia a productos Google y Microsoft

*Eduard Chaveli Donet, Socio Director de GESDATOS*

GESDATOS
SOFTWARE DE PROTECCIÓN DE DATOS

# 1. INTRODUCCIÓN.

## CLOUD COMPUTING EXIGE ANÁLISIS DE RIESGOS

## VENTAJAS / RIESGOS:

- Reputación
- Económico: pérdidas, sanciones, costes litigios …
- Rechazo (Ej. publicidad contextual en determinados servicios)

Muchas veces los riesgos están relacionados con el cumplimiento o incumplimiento de **aspectos legales**…

## 2. ASPECTOS LEGALES

### 2.1. VISIÓN GENERAL

Entre otros:

► Aspectos generales derivados del Outsourcing (especialmente responsabilidad).

► Ubicación territorial: legislación aplicable, jurisdicción, LOPD…

### 2.2. ASPECTOS RELATIVOS A LA RESPONSABILIDAD

*Responsabilidad = diversas consecuencias:*

*Económicas - se pueden mitigar o desplazar (ej. Contrato de Seguros, Repercutir al proveedor)*

Los contratos suelen disponer de:

- Cláusulas de exclusión de responsabilidad a ciertos supuestos
- Cláusulas de limitación de la responsabilidad.

Ejemplos de Cláusulas de limitación de Google:

> *"… la responsabilidad de cada parte derivada del presente Contrato (de carácter contractual, extracontractual o de cualquier otra naturaleza) resultante de cualesquiera hechos o circunstancias o serie de hechos o circunstancias relacionadas entre sí estará limitada al mayor de los siguientes importes: (a) un 125% de la totalidad de los importes debidos y satisfechos por el Cliente en virtud del presente Contrato durante los 12 últimos meses anteriores al mes en el que el hecho o serie de hechos en cuestión hubieran tenido lugar; o (b) 25.000 Euros".*

Es decir: según estas cláusulas:

- Se limita la responsabilidad a una serie de supuestos.
- Y en el caso de que exista está limitada.

# CONSEJO 1

## Revisar las causas de exclusión de responsabilidad y los límites de exclusión de responsabilidad.

## 2.3. ESPECIAL REFERENCIA A LA PRIVACIDAD (PROTECCIÓN DE DATOS)

## 2.3.1. INTRODUCCIÓN

¿Hay tratamiento de datos personales y por tanto es de aplicación la legislación sobre protección de datos?

La aplicación de la norma no únicamente cuando se aloje una BBDD.

A tener en cuenta:

**1. El estándar de exigencia fijado por el TJCE en el Asunto C-101, Lindqvist, es muy alto:**

*«… la conducta que consiste en hacer referencia, en una página web, a diversas personas y en identificarlas por su nombre o por otros medios, como su número de teléfono o información relativa a sus condiciones de trabajo y a sus aficiones, constituye un «tratamiento total o parcialmente automatizado de datos personales»*

**2. El concepto de dato de carácter personal es amplio** (según AEPD):

1. Persona identificada: nombre y apellidos, imagen …
2. Pero también identificable: DNI, IP, email, matrícula de vehículo….

**3. En particular:**

1. En el caso de provisión de servicios de correo electrónico
La asignación de cuentas de correo = tratamiento de DP.

2. La contratación del uso de aplicaciones que potencialmente, sirvan para el tratamiento de datos personales = tratamiento de DP.

# CONSEJO 2

## Revisar si el servicio prestado supone un tratamiento de datos, teniendo en cuenta el concepto amplio de datos personales

## *2.3.2. DERECHO APLICABLE EN PROTECCIÓN DE DATOS*

### ¿Aplica la legislación española?

Artículo 2 LOPD y 3 del RDLOPD.

Se regirá aplicará la legislación española de protección de datos cuando:

• **El responsable del tratamiento: en territorio español.**
Aplican todas las obligaciones de la LOPD y del RD 1720/2007.

• El encargado del tratamiento: en España.
Serán de aplicación al mismo las medidas de seguridad (título VIII del RD 1720/2007).
• El responsable del tratamiento no en territorio español, pero aplicación legislación española, según Derecho internacional público.
• El responsable del tratamiento no en UE pero utilice medios situados en España, salvo medios de tránsito.
El responsable deberá designar un representante en España.

**Por tanto: los asistentes a esta jornada en tanto en cuanto sus organizaciones son responsables y contraten servicios en régimen de cloud, (independientemente de quien sea el proveedor y donde esté) han de cumplir con las obligaciones de la LOPD y del RD 1720/2007**

# CONSEJO 3

## Tener en cuenta que la legislación aplicable en privacidad a nuestras organizaciones es la española

## *2.3.3. ENCARGADO DEL TRATAMIENTO*

## *A.* CONCEPTO

El encargado del tratamiento se define por el art. 5 RDLOPD en los siguientes términos:

*«Encargado del tratamiento: La persona física o jurídica, pública o privada, u órgano administrativo que, solo o conjuntamente con otros, trate datos personales* ***por cuenta del responsable*** *del tratamiento o del responsable del fichero, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación* ***para la prestación de un servicio».***

Conclusión: el prestador de servicios en la Nube es un encargado del tratamiento.

Consecuencia: aplicación del conjunto de criterios del Capítulo III del Título II del RD 1720/2007.

## B. OBLIGACIÓN: FIRMA DE UN CONTRATO

• La LOPD (art. 12) exige **que se firme un contrato** entre el Responsable del fichero y el encargado del tratamiento que regule las condiciones en que dicho tercero va a tratar los datos.

• En la práctica **formalmente** puede consistir:
• bien en un contrato *ad hoc*,
• en una cláusula del contrato de prestación de servicios de que se trate,
• o en un anexo a dicho contrato.

### Contenido obligatorio

• "*que el encargado del tratamiento únicamente tratará los datos conforme a las **instrucciones** del responsable*"
• "*que **no los aplicará o utilizará** con un **fin distinto** al que figure en dicho contrato*".
• *"que **no los comunicará,** ni siquiera para su conservación, a otras personas*".
• *"las **medidas de seguridad …** que el encargado del tratamiento está obligado a implementar".*
• *"que **una vez cumplida la prestación** contractual, los datos de carácter personal deberán ser **destruidos o devueltos** al responsable del tratamiento …"*

## ¿QUÉ TENEMOS QUE COMPROBAR?:

¿Cómo se contrata: podemos negociar algunos términos del contrato?

¿Está dispuesto a aceptar las exigencias dimanantes de la legislación española como encargado?

¿Reúne el contrato las condiciones del artículo. 12 LOPD (contenido obligatorio) aunque sea de forma “dispersa”?

Ejemplo: En el caso de Google el contenido del art. 12 de la LOPD no se halla en una única cláusula.

> 1.Protección de Datos. A efectos de lo dispuesto en la Cláusula 1.4 y la presente Cláusula 1.5, las expresiones “datos de carácter personal", “tratamiento”, “responsable del tratamiento” y “encargado del tratamiento” tendrán el significado que en cada caso se atribuye a las mismas en la Directiva**.** A los efectos del presente Contrato, y respecto de los datos de carácter personal de los Usuarios, las partes acuerdan que el Cliente y Google tendrán la condición de, respectivamente, responsable y encargado del tratamiento. Google adoptará e implantará las correspondientes medidas técnicas y organizativas necesarias a efectos de proteger dichos datos de carácter personal de su destrucción o pérdida, alteración, acceso o revelación no autorizada, en cada caso de carácter accidental o negligente.

# C. ASPECTOS CONCRETOS

## 1.SUBCONTRACIÓN

**A. Regla general:** "El encargado del tratamiento no podrá subcontratar…"
**B. Régimen alternativo:** posibilidad de subcontratación cuando hubiera obtenido de éste autorización para ello. Requisitos:

A. Se especifiquen en el contrato los servicios que puedan ser objeto de subcontratación y, si ello fuera posible, la empresa con la que se vaya a subcontratar.

B. Cuando no se identificase en el contrato la empresa con la que se vaya a subcontratar, será preciso que el encargado del tratamiento comunique al responsable los datos que la identifiquen antes de proceder a la subcontratación.

C. Que el tratamiento de datos de carácter personal por parte del subcontratista se ajuste a las instrucciones del responsable del fichero.

D. Que el encargado del tratamiento y la empresa subcontratista formalicen el contrato del art. 12 LOPD.

Si se da una subcontratación sobrevenida total o parcial no prevista en el contrato: debe someterse al responsable.

## ¿ QUÉ TENEMOS QUE COMPROBAR ?

1. ¿El encargado subcontrata y se le autoriza?

2. ¿Se cumplen los requisitos indicados (letras A – D)?

Ejemplo contrato incorrecto de Google:

1.~~Sub-contratación. Cualquier parte podrá subcontratar total o parcialmente el cumplimiento de sus obligaciones derivadas del presente Contrato sin necesidad de obtener el previo consentimiento por escrito de la otra parte. La parte que hubiera subcontratado el cumplimiento de sus obligaciones continuará no obstante siendo plenamente responsable del cumplimiento de las mismas, en particular por cualesquiera acciones y/u omisiones de sus subcontratistas al respecto, tal y como si se tratara de sus propias acciones y/o omisiones.~~

## 2. EL DEBER DE VIGILANCIA DEL RESPONSABLE EN RELACIÓN CON EL ENCARGADO

**Art. 20 RDLOPD**: "Cuando el responsable del tratamiento contrate la prestación de un servicio que comporte un tratamiento de datos personales sometido a lo dispuesto en este Capítulo deberá **velar por que el encargado del tratamiento reúna las garantías** para el cumplimiento de lo dispuesto en este Reglamento".

**CUESTIÓN:** ¿Cuándo se puede entender que el responsable "cumple" y no será responsable de los actos del encargado?

Algunas soluciones a este deber de vigilancia:

**1.** La diligencia deberá estar relacionada con el tratamiento que se le encomienda al tercero: medidas de seguridad/obligaciones jurídicas.

**2.** Forma: Cláusula que habilite al responsable a solicitar documentación al encargado: ej. Informe de auditoría, documento de seguridad etc…

## 3. SEGURIDAD

1. Si el encargado está en la UE: con el estándar del País es suficiente.

2. Si no está en la UE: pactar el RDLOPD

Artículo 82 RDLOPD

*3. En todo caso, el acceso a los datos por el encargado del tratamiento estará sometido a las medidas de seguridad contempladas en este reglamento.*

# ¿QUÉ TENEMOS QUE COMPROBAR?

1. Los niveles establecen un mínimo: nada impide un plus de exigencia.

2. En general: ¿ hemos realizado un mínimo análisis de riesgos? ¿Se nos ofrece información fiable?

3. Elementos básicos:
   1. Formación de los usuarios del encargado.
   2. Copias de seguridad.
   3. Protección de los accesos a través de redes.
   4. Protocolos de gestión y respuesta ante incidencias.
   5. Controles de acceso y protección frente accesos indebidos de otros clientes y terceros proveedores.
   6. Localización de los recursos.
   7. Identificación y autenticación.
4. ¿Reúne el software los requisitos de la Disp. Ad. Primera?
5. ¿Dispone de alguna certificación o emplea alguna métrica que podamos verificar? ¿ISO 27001?
6. ¿Se audita? Y si lo hace ¿Exhibe documentación acreditativa y fiable?

Alguna de las cuestiones planteadas, tienen respuesta para el caso del proveedor de servicios SalesForce.com en su política de privacidad disponible en su web: http://www.salesforce.com/company/privacy.jsp Por ejemplo, en respuesta al punto 4. la empresa proveedora de servicios dispone de certificaciones tales como: ISO 27001, SAS 70 Type II y Systrust.

# 4. CONSERVACIÓN DE LOS DATOS POR EL ENCARGADO

Ya previsto y regulado en la LOPD en los siguientes términos:

• **Art.12.3:** "Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento".

Previsión avanzada pero insuficiente. Por ello el art. 22 RDLOPD:

- **Añade** la posibilidad de **devolución de los datos al encargado que el Responsable hubiese designado**.

- **Esclarece** la disyunción entre "**destruidos o devueltos**".

"*No procederá la destrucción … cuando exista una previsión legal que exija su conservación, en cuyo caso deberá procederse a la devolución de los mismos garantizando el responsable del fichero dicha conservación*".

- **Establece posibilidad encargado conserve** datos para salvar responsabilidades

Informe 283/2004. Conservación de los datos por el encargado del tratamiento

Ejemplo de previsión en los contratos de Google:

1.Efectos de la resolución del Contrato. En caso de resolución del presente Contrato (incluyendo en el supuesto de resolución de las Órdenes de Pedido): (i) decaerán inmediatamente cualesquiera derechos otorgados por cualquiera de las partes a la otra; (ii) Google **permitirá al Cliente acceder y exportar** los Datos del Cliente **durante un período razonable de tiempo,** a las tarifas de Google vigentes en ese momento respecto de los Servicios aplicables en cuestión; (iii) **transcurrido dicho período razonable, Google borrará los Datos del Cliente** de conformidad con las Políticas de Privacidad de Google; (iv) cada parte, a solicitud de la otra, devolverá o destruirá inmediatamente cualquier Información Confidencial de esta última que se encontrase en su poder.

# CONSEJO 4

## Revisar que se contemplen específicamente las previsiones generales respecto del encargado y las específicas:

- Previsiones de subcontratación.
- Deber de diligencia
- Medidas de seguridad
- Asegurar la conservación y pacífica exportación de datos

## *2.3.4. TRANSFERENCIAS INTERNACIONALES DE DATOS (TID)*

### A.CONCEPTO

• **Transferencia Internacional de datos** (artículo 5.1.s RLOPD)

Tratamiento de datos que supone la transmisión de los datos fuera del Espacio Económico Europeo, tanto cesión (a otro responsable) tanto prestación de un servicio (encargado de tratamiento)

Transmisión de datos a países del Espacio Económico Europeo = NO TID
SI posible **Cesión de Datos**

## B. MARCO REGULADOR

- **DIRECTIVA 95/46 DE PROTECCIÓN DE DATOS. Arts. 25 y 26**

- **LOPD. Arts. 33 y 34**

- **REGLAMENTO DE DESARROLLO LOPD. RD 1720/2007**
  - ❑Título VI. Transferencias Internacionales de datos.
  - ❑Título IX. Capítulo V. Procedimientos relacionados con las transferencias internacionales de datos.

- **DECISIONES COMISIÓN EUROPEA**

http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/union_europea/decisiones/index-ides-idphp.php

- **Especialmente:**

Decisión de la Comisión (2010/87/UE), de 5 de febrero de 2010, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo.

## C. RÉGIMEN. OPCIONES. VISIÓN GENERAL

### 1. DENTRO DEL ESPACIO ECONÓMICO EUROPEO

No TID

### 2. A PAÍS CON NIVEL ADECUADO DE PROTECCIÓN

Si TID pero sólo requiere comunicarla en la Inscripción

### 3. ESTADOS QUE NO PROPORCIONAN NIVEL ADECUADO DE PROTECCIÓN

Si TID y además requiere autorización del Director de la Agencia Española de Protección de Datos (art. 70 RLOPD)

## D. DETALLE

## 1. ESPACIO ECONÓMICO EUROPEO

- **NO TDI**
- Posible:

A) Cesión de datos

B) Prestación de servicios - Encargado de tratamiento (art. 12 LOPD, arts. 20-22 RLOPD)

- Exigencias: LOPD ↔ Directiva 95/46/CE

## 2. NIVEL ADECUADO DE PROTECCIÓN

### SI TDI

• **Decisión de adecuación de la Comisión Europea (art. 68 RLOPD)**
Suiza, Argentina, Guernsey, Man, Jersey, Islas Feroe, Canadá, Israel, Andorra

**EEUU:** Safe Harbor

Web:
http://www.export.gov/safeharbor/

Listado:
https://safeharbor.export.gov/list.aspx

Ejemplos: Microsoft, Amazon, Google…

- Solo es precisa la comunicación de las Transferencias Internacionales en la notificación del fichero. No necesaria autorización
- Y las exigencia derivadas de la Cesión o encargado de tratamiento

## 3. ESTADOS QUE NO PROPORCIONAN NIVEL ADECUADO DE PROTECCIÓN

- **SI TDI**

- **Necesaria autorización del Director de la Agencia Española de Protección de Datos (art. 70 RLOPD)**

- Necesario contemplar las **decisiones de la Comisión y** que el contrato tenga el contenido de las **cláusulas contractuales tipo**,

No son “copia pega” sino que han de revisarse y adaptarse a medida; y se ha de verificar exactamente los países de alojamiento.

Relación de autorizaciones. Publicadas en:

https://www.agpd.es/portalwebAGPD/resoluciones/autorizacion_transf/index-ides-idphp.php

# CONSEJO 5

## Tener claro el escenario aplicable a las TID y si se cumplen las exigencias de la misma

# 3. E.N.S. – ESQUEMA NACIONAL DE SEGURIDAD

Categorización de los Sistemas de Información:

**Nivel BAJO.**

Se utilizará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un **perjuicio limitado sobre las funciones de la organización**, sobre sus activos o sobre los individuos afectados.

Se entenderá por perjuicio limitado:

1.º La **reducción de forma apreciable de la capacidad de la organización para atender eficazmente con sus obligaciones corrientes**, aunque estas sigan desempeñándose.
2.º El sufrimiento de un daño menor por los activos de la organización.
3.º El **incumplimiento formal de alguna ley o regulación, que tenga carácter de subsanable**.
4.º Causar un perjuicio menor a algún individuo, que aún siendo molesto pueda ser fácilmente reparable.
5.º Otros de naturaleza análoga.

## Nivel MEDIO

Se utilizará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un **perjuicio grave sobre las funciones de la organización**, sobre sus activos o sobre los individuos afectados.

Se entenderá por perjuicio grave:

1.º La **reducción significativa la capacidad de la organización para atender eficazmente a sus obligaciones fundamentales**, aunque estas sigan desempeñándose.
2.º El sufrimiento de un daño significativo por los activos de la organización.
3.º El **incumplimiento material de alguna ley o regulación, o el incumplimiento formal que no tenga carácter de subsanable**.
4.º Causar un perjuicio significativo a algún individuo, de difícil reparación.
5.º Otros de naturaleza análoga.

## Nivel ALTO

Se utilizará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un **perjuicio muy grave sobre las funciones de la organización**, sobre sus activos o sobre los individuos afectados.

Se entenderá por perjuicio muy grave:
1.º La **anulación de la capacidad de la organización para atender a alguna de sus obligaciones fundamentales y que éstas sigan desempeñándose**.
2.º El sufrimiento de un daño muy grave, e incluso irreparable, por los activos de la organización.
3.º El **incumplimiento grave de alguna ley o regulación**.
4.º Causar un perjuicio grave a algún individuo, de difícil o imposible reparación.
5.º Otros de naturaleza análoga.

### 4.1.3 Adquisición de nuevos componentes [op.pl.3].

| dimensiones | todas | | |
|---|---|---|---|
| categoría | básica | media | alta |
| | aplica | = | = |

Se establecerá un proceso formal para planificar la adquisición de nuevos componentes del sistema, proceso que:

a) Atenderá a las conclusiones del análisis de riesgos: [op.pl.1].
b) Será acorde a la arquitectura de seguridad escogida: [op.pl.2].
c) Contemplará las necesidades técnicas, de formación y de financiación de forma conjunta.

### 4.4.3 Medios alternativos [op.ext.9].

| dimensiones | D | | |
|---|---|---|---|
| nivel | bajo | medio | alto |
| | no aplica | no aplica | aplica |

Estará prevista la provisión del servicio por medios alternativos en caso de indisponibilidad del servicio contratado. El servicio alternativo disfrutará de las mismas garantías de seguridad que el servicio habitual.

### 5.8.1 Protección del correo electrónico (e-mail) [mp.s.1].

| dimensiones | todas | | |
|---|---|---|---|
| categoría | básica | media | alta |
| | aplica | = | = |

El correo electrónico se protegerá frente a las amenazas que le son propias, actuando del siguiente modo:

a) La información distribuida por medio de correo electrónico, se protegerá, tanto en el cuerpo de los mensajes, como en los anexos.

b) Se protegerá la información de encaminamiento de mensajes y establecimiento de conexiones.

c) Se protegerá a la organización frente a problemas que se materializan por medio del correo electrónico, en concreto:

1.º Correo no solicitado, en su expresión inglesa «spam».

2.º Programas dañinos, constituidos por virus, gusanos, troyanos, espías, u otros de naturaleza análoga.

3.º Código móvil de tipo «applet».

d) Se establecerán normas de uso del correo electrónico por parte del personal determinado. Estas normas de uso contendrán:

1.º Limitaciones al uso como soporte de comunicaciones privadas.

2.º Actividades de concienciación y formación relativas al uso del correo electrónico.

### 5.8.2 Protección de servicios y aplicaciones web [mp.s.2].

| dimensiones | todas | | |
|---|---|---|---|
| categoría | básica | media | alta |
| | aplica | = | = |

Los subsistemas dedicados a la publicación de información deberán ser protegidos frente a las amenazas que les son propias.

a) Cuando la información tenga algún tipo de control de acceso, se garantizará la imposibilidad de acceder a la información obviando la autenticación, en particular tomando medidas en los siguientes aspectos:

1.º Se evitará que el servidor ofrezca acceso a los documentos por vías alternativas al protocolo determinado.
2.º Se prevendrán ataques de manipulación de URL.
3.º Se prevendrán ataques de manipulación de fragmentos de información que se almacena en el disco duro del visitante de una página web a través de su navegador, a petición del servidor de la página, conocido en terminología inglesa como «cookies».
4.º Se prevendrán ataques de inyección de código.

b) Se prevendrán intentos de escalado de privilegios.
c) Se prevendrán ataques de «cross site scripting».
d) Se prevendrán ataques de manipulación de programas o dispositivos que realizan una acción en representación de otros, conocidos en terminología inglesa como «proxies» y, sistemas especiales de almacenamiento de alta velocidad, conocidos en terminología inglesa como «cachés».

Disponemos de un grupo en Linkedin, donde se abordan temas referentes al Esquema Nacional de Seguridad.
Se organizan debates donde profesionales en la materia solucionan dudas y cuestiones acerca del mismo.

El grupo se llama: “ENS – Esquema Nacional de Seguridad ”

# MUCHAS GRACIAS

902 900 231

info@gesdatos.com

www.gesdatos.com

GES DATOS

SOFTWARE DE PROTECCIÓN DE DATOS