Hacia la seguridad de los datos

José Luis Rivas (jlrivas@uvigo.es) @jlrivas

Victor Salgado (v.salgado@udc.es) @abonauta

EuroPriSe European Privacy Seal

Universidade de Vigo

UNIVERSIDADE DA CORUÑA

José Luis Rivas López

- Participante en diversas comunidades y grupos de trabajo:
  - Europrise (Experto por UE DE 95/46/CE), ANAFON, etc.
- Ponente invitado en diversas conferencias, seminarios y cursos de master nacionales e internacionales:
  - RedIRIS JT/GT, Cursos de Postgrado, Microsoft, etc.
- Miembro de Jurados Internacional del Reto de Análisis Forense
- Vocal del AEN/CTN 197 (Computing and Networking Forensic Reports) - AENOR
- Auditor jefe e Implantador ISO 27001 y 22301 por AENOR
- Miembro del comité de acreditación EURO-INF de ANECA
- Solicitud de patentes:
  - Abril 2013: "Sistema de guarda, salvaguarda y gestión de evidencias digitales validas" (P201300340)
  - Abril 2002: "Dispositivo de interacción táctil de elementos no textuales para personas con deficiencias visuales" (P200200869)
  - Octubre 2001: "Sistemas de detección de bombas lapas en vehículos (S.A.L.)" (P200102223)
- Autor de 10 libros y articulos en diferentes revistas técnicas:
  - 2015/16 Sistemas de automatización y autómatas programables (en proceso de publicación)
  - 2015 El nuevo procedimiento administrativo local tras la Ley 39/2015 (I.S.B.N. 978-84-7052-713-5)
  - 2010: Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal (I.S.B.N. 978-84-470-3423-9)
  - 2009: Introducción al analisis forense
  - 2004: Implementación de la ley de protección de datos (I.S.B.N.: 84-95660-91-1)
  - 2003: Protección de datos (I.S.B.N.: 84-95660-89-X)
  - 2003: Seguridad Técnica y Legal (I.S.B.N.: 84-95660-88-1)
- 1 premio al mejor invento y 1 nominación por el club de inventores

Víctor A. Salgado Seguín

- ***Socio Director de Pintos & Salgado Abogados, especializado desde sus inicios en Derecho Informático y Comunitario y autor del blog "Abonauta", nominado para el Premio al mejor Blog Jurídico 2010 por Derecho en Red y la Editorial Bosch.***
- ***Licenciado en Derecho y Diplomado Superior en Gestión Empresarial por la Universidad CEU San Pablo de Madrid y primera promoción del Máster en Estudios de la Unión Europea de la Universidad de A Coruña. Su tesis de Licenciatura se centró en los "Aspectos Jurídico-comunitarios sobre Internet: La Sociedad de la Información" obteniendo la Suficiencia Investigadora como Doctorando en la misma Universidad.***
- ***Profesor de Derecho Informático en la Facultad de Derecho de la Universidad de A Coruña, es también socio-fundador del Capítulo Gallego de la Internet Society (ISOC- GAL).***
- ***En el año 2000 fue incluido en las listas de Expertos de la Comisión Europea para evaluar Proyectos de I+D relacionados con la Sociedad de la Información.***
- ***Ha obtenido el "EuroPriSe Legal Expert Certificate" del primer sello de Privacidad Europeo auspiciado por la Comisión Europea en 2008 y ha sido reconocido con el "European Certificate on CiberCrime and e- Evidence" o Certificado Europeo en Cibercrimen y Prueba Electrónica, auspiciado igualmente por la Unión Europea.***
- ***Ha publicado una veintena de artículos en boletines y revistas especializadas, tanto a nivel nacional como internacional, sobre Aspectos Jurídicos del Comercio Electrónico, la legislación en materia de Protección de Datos, los Derechos de Autor en Internet, la Criminalidad Informática o la regulación de los Nombres de Dominio, entre otras.***
- ***Ponente en más de un centenar de conferencias académicas y profesionales sobre distintos ámbitos relacionados con el Derecho Informático e Internet.***
- ***Asimismo, es socio fundador de la "Asociación de Expertos Nacionales de la Abogacía TIC" (ENATIC).***

OBJETIVOS

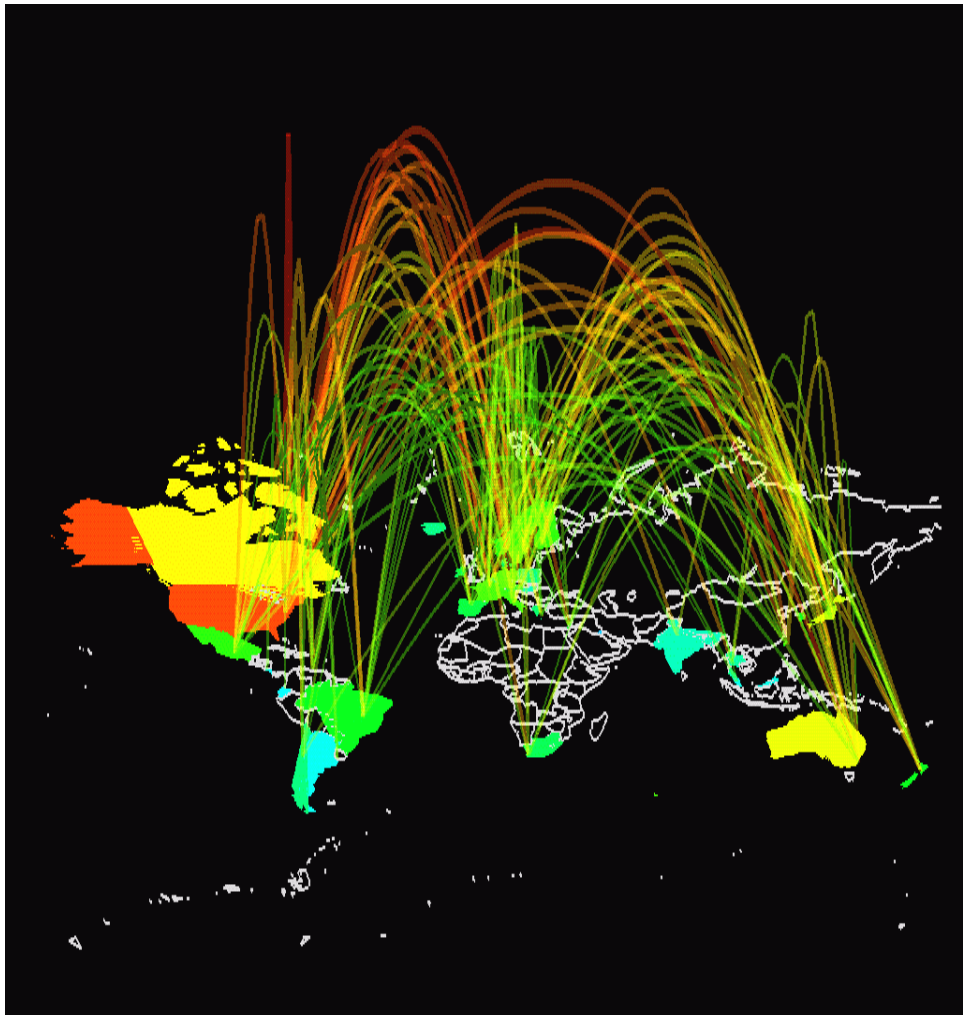
Conocer todo aquello relativo al nuevo marco normativo referente a la privacidad y protección de datos.

- ***Teléfonos móviles***

Agenda

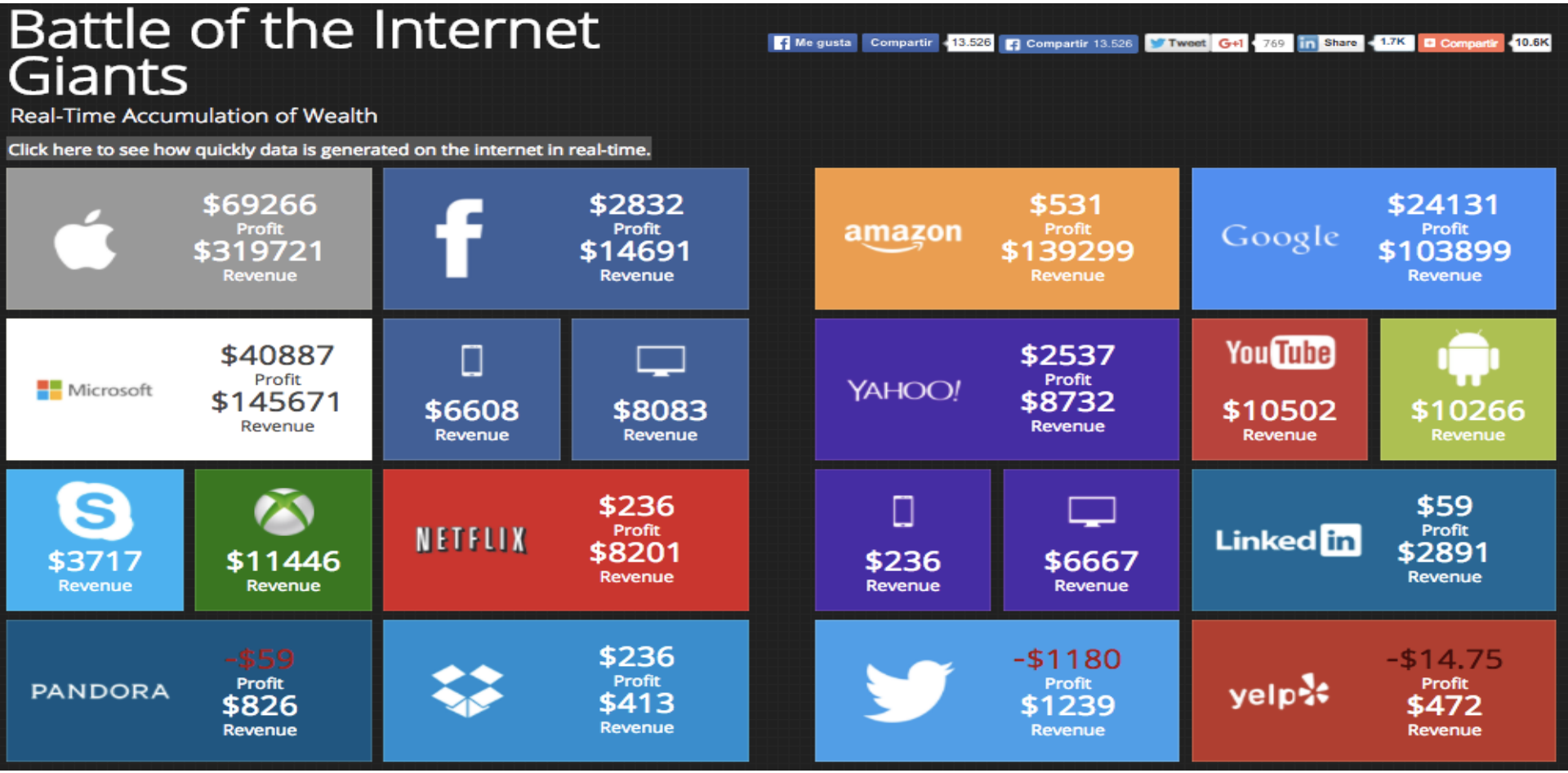
- Introducción
- Definiciones
- Cambios
- Análisis de Riegos, DPO, derechos, incidentes, etc.
- Preguntas

Internet



Internet en tiempo real

http://pennystocks.la/battle-of-internet-giants/



Objetivos que pretende la UE

- ***Abordar el impacto de las NNTT***
- ***Aumentar la transparencia***
- ***Sensibilización***
- ***Garantizar el consentimiento***
- ***Sensibilización***

INTRODUCCIÓN
ÁMBITO LEGAL EN PROTECCIÓN DE DATOS

Antecedentes a la Legislación vigente

- Declaración de Derechos Humanos (1948)
- Directrices Básicas Consejo de Europa (1973-74)
- Artículo 18 de la **Constitución Española** (1978)

  ……..La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.
- Ley Orgánica 5/1992 de regulación del tratamiento automatizado de los DCPs. **(LORTAD)** - ***Derogada por la LOPD***
- **DIRECTIVA 95/46/CE** DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de éstos – **Derogada por RGPD**
- **Carta de Derechos Fundamentales de la Unión Europea** (Art. 8)
- RD 994/1999 (RMS) - **Derogada por RDLOPD**

Sentencia del Tribunal Constitucional 292/2000

La protección de los datos personales es un **derecho fundamental** que afecta a cualquier tipo de dato, sea íntimo o no. Se tiene un **derecho de control** sobre los datos relativos a la propia persona

Reglamento UE 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (RGPD)

La **Ley Orgánica 15/1999, de 13 de diciembre, de Protección de los DCPs (LOPD)** culmina los desarrollos legales en materia de protección de datos.

El **RD 1720/2007, constituye el marco regulatorio de seguridad de los DCPs**

Definiciones

Nuevas definiciones, a destacar:

<u>Dato personal</u>: «toda información sobre una persona física identificada o identificable…»

Art. 2.2 RDLOPD: «Este reglamento no será aplicable […], ni a los ficheros que se limiten a incorporar los datos de las personas físicas que presten sus servicios en aquéllas, consistentes únicamente en su nombre y apellidos, las funciones o puestos desempeñados, así como la dirección postal o electrónica, teléfono y número de fax profesionales.»

Art. 2.3 RDLOP: «Asimismo, los datos relativos a empresarios individuales, cuando hagan referencia a ellos en su calidad de comerciantes, industriales o navieros, también se entenderán excluidos del régimen de aplicación de la protección de datos de carácter personal.»

Definiciones

Nuevas definiciones, a destacar:

Datos biométricos y genéticos: ahora son datos especialmente protegidos. Atención porque la imagen de la persona puede pasar a ser dato especialmente protegido.

Igualmente los datos dactiloscópicos.

Seudonimización: situación intermedia entre el dato personal íntegro y el anonimizado. Especial relevancia para el análisis de riesgos.

Datos biométricos

Tecnología	Dispositivos de captura
Huella dactilar	Periférico de escritorio o lector integrado
Reconocimiento de voz	Micrófono
Reconocimiento de escritura del teclado	Teclado
Reconocimiento de firma	Tableta y puntero/bolígrafo para firmar
Reconocimiento de iris	Cámara infrarrojos
Reconocimiento facial	Cámara
….	….

Categorías especiales de Datos

Prohibición de tratamiento (salvo excepciones)

- **Origen racial o étnico**
- **Opiniones políticas**
- **Creencias religiosas o filosóficas**
- **Pertenencia a sindicatos**
- **Tratamiento datos genéticos**
- **Biométricos**
- **Datos de salud**
- **Orientación sexual**

El Consentimiento

El consentimiento tácito desaparece (no valido deducido del silencio o de la inacción de los ciudadanos)

El consentimiento debe ser una manifestación de voluntad:

* *Libre*
* *Específica*
* *Informada*
* *Inequívoca*

CONSENTIMIENTO DEMOSTRABLE

- ***** Inequívoco = declaración de los interesados o una acción que indique el acuerdo del interesado***

Avisos Legales/ Cláusulas

Nuevo contenido del deber de información. Ahora hay que informar de algunas cosillas más:

1. *la identidad y los datos de contacto del responsable y, en su caso, de su representante;*
2. *los datos de contacto del delegado de protección de datos, en su caso;*
3. *los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento;*
4. *cuando el tratamiento se base en el artículo 6, apartado 1, letra f), los intereses legítimos del responsable o de un tercero;*
5. *los destinatarios o las categorías de destinatarios de los datos personales, en su caso;*
6. *en su caso, la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al hecho de que se hayan prestado.*
7. *el plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo;*
8. *la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;*
9. *cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada; d) el derecho a presentar una reclamación ante una autoridad de control;*
10. *si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de que no facilitar tales datos;*
11. *la existencia de decisiones automatizas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.*

Avisos Legales/ Cláusulas

Información al titular cuando los datos no han sido recabados directamente de él:

El plazo actual se reduce de 3 meses a máximo 1 mes.

Se exceptúa expresamente el informar cuando existe un deber de secreto profesional.

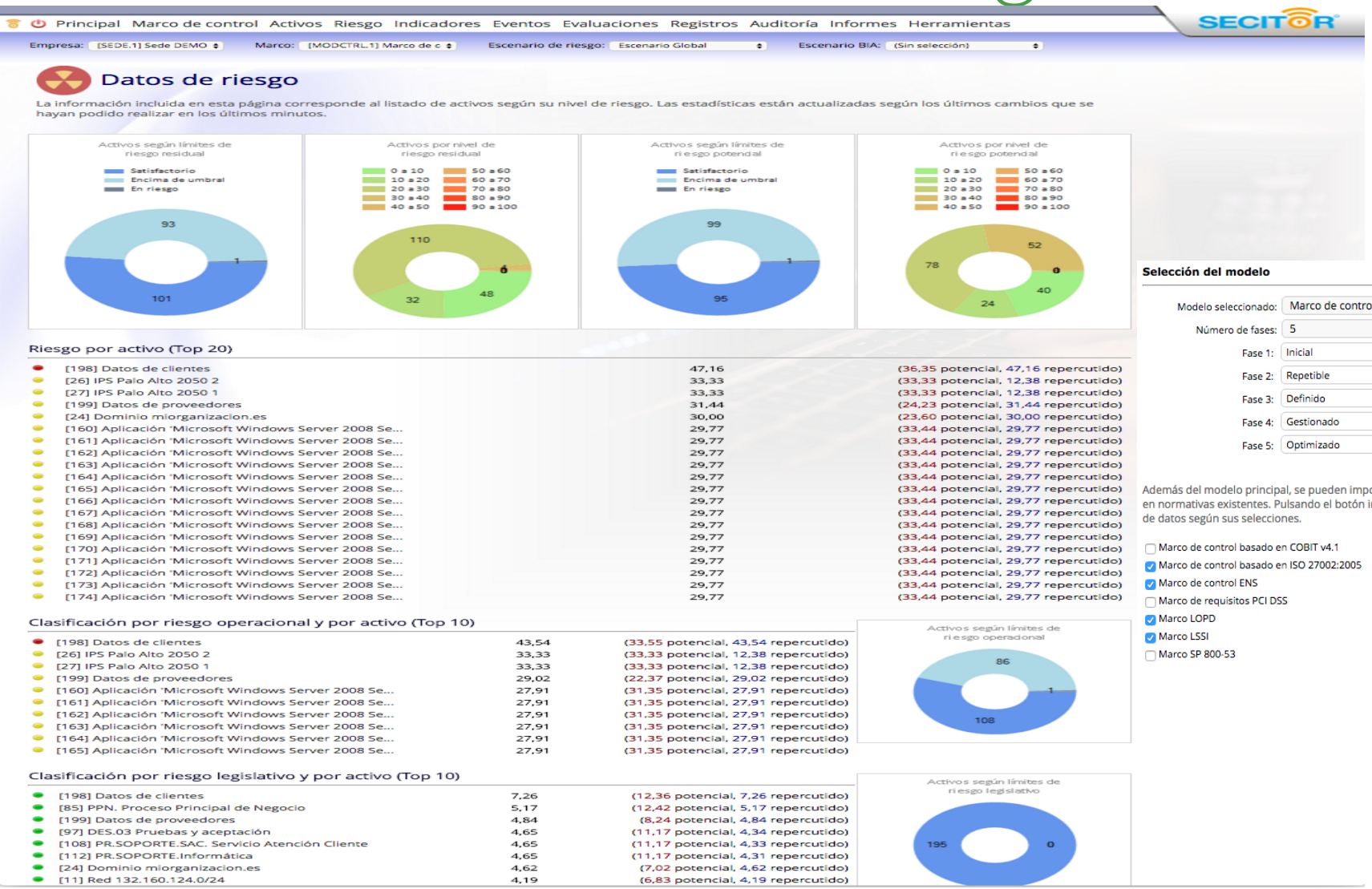
Responsabilidad Proactiva

Medidas que aseguren razonablemente que están en condiciones de cumplir con los principios, derechos y garantías que el Reglamento establece:

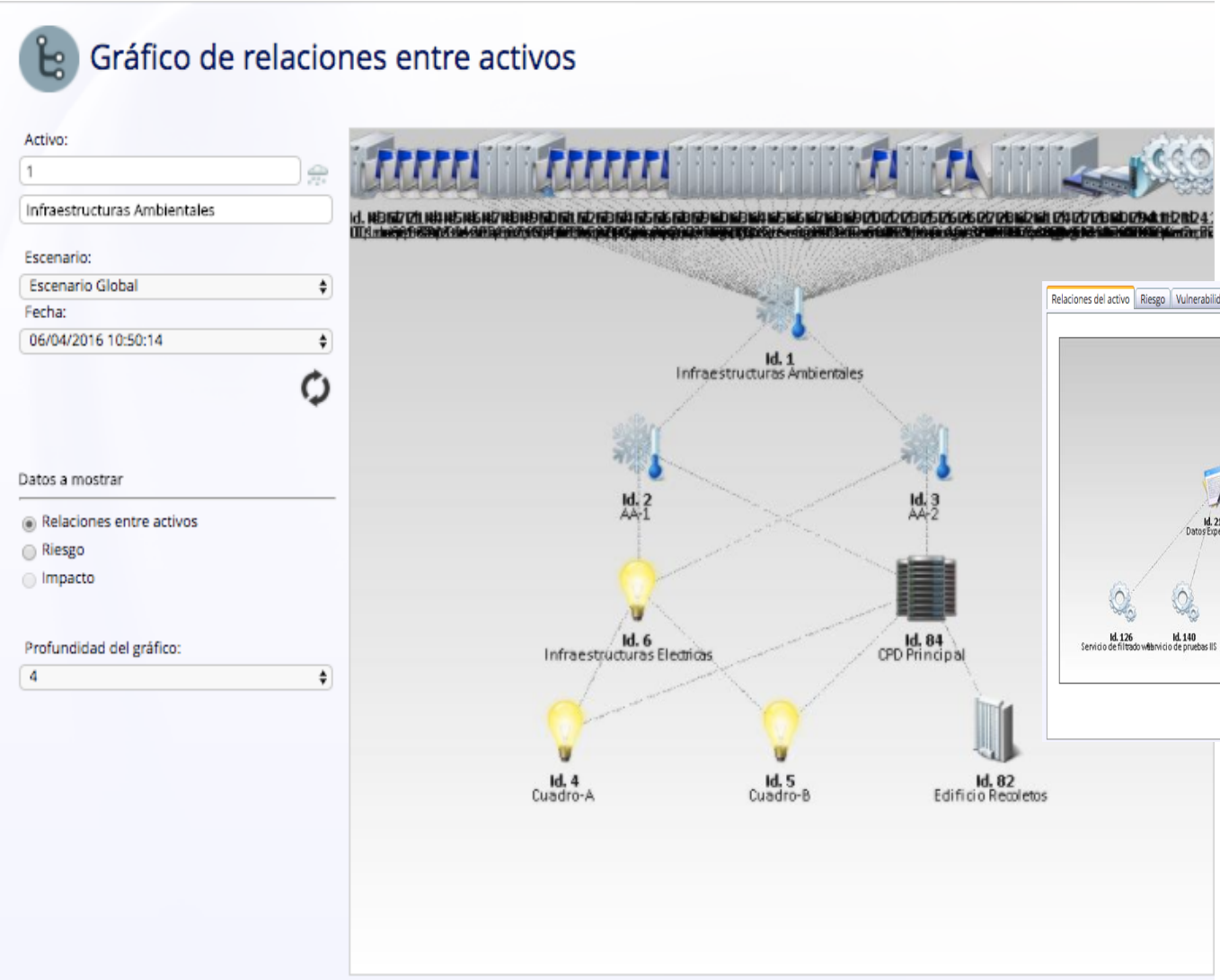
- *Protección de datos desde el diseño*
- *Protección de datos por defecto*
- *Medidas de seguridad*
- *Mantenimiento de un registro de tratamientos*
- *Realización de evaluaciones de impacto sobre la protección de datos*
- *Nombramiento de un delegado de protección de datos*
- *Notificación de violaciones de la seguridad de los datos*

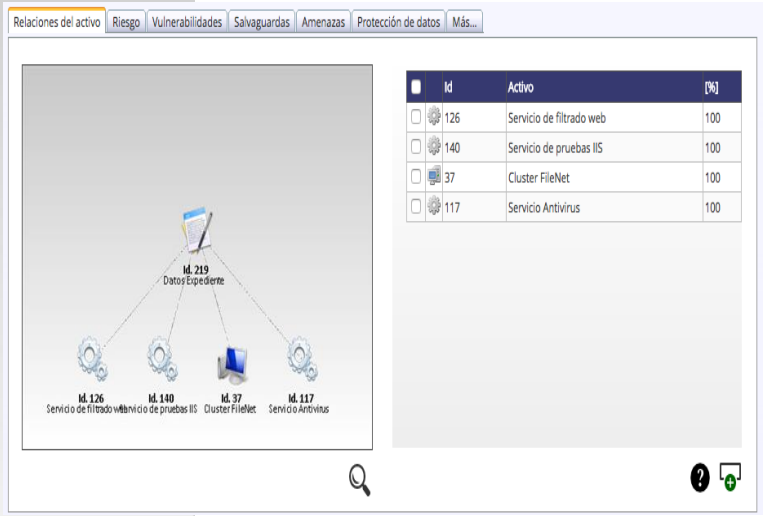
EL ANÁLISIS DE RIESGOS

Análisis de Riesgos



Análisis de Riesgos





Notificaciones de Violaciones de Seguridad

72 horas máximo para notificar violaciones de seguridad a la Autoridad de Control.

También notificación a los afectados, excepciones:

- *Cuando la quiebra no entrañe alto riesgo para sus derechos y libertades.*
- *Cuando antes de la quiebra se hubieran implementado medidas de protección tecnológica como el cifrado de la información.*

Los Registros de Ficheros

Desaparece la obligación de inscribir ficheros.

Ahora hay una obligación de registro interno de tratamientos.

Derecho de Acceso

Se amplía la información que el interesado tiene derecho a recibir, por ejemplo:

- *Plazos de conservación de los datos.*
- *El derecho a presentar una reclamación ante la autoridad de control.*

Se deberá responder por vía electrónica.

Posibilidad de pagar un canon por recibir copias adicionales.

Derecho de Supresión

(«derecho al olvido», MAL LLAMADO)

Obligación de suprimir los datos personales cuando concurran algunas de las circunstancias que menciona el Reglamento.

Excepción: cuando nos encontremos ante el ejercicio del derecho a libertad de información o expresión.

Derecho de Limitación del Tratamiento

Marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro.

Es una «cancelación o bloqueo cautelar».

Derecho de Oposición

Novedad: se invierte la carga de la prueba. Ahora es el responsable del tratamiento el que tiene que probar un interés legítimo superior al derecho del afectado a que se supriman sus datos.

Derecho de Portabilidad

Derecho del interesado de recibir copia o de que sus datos sean trasladados de un responsable a otro, cuando «sea técnicamente posible».

¿Quién decide que es es técnicamente posible?

Relación
Responsable <-> Encargado

Se mantiene la formalidad de la existencia de un contrato.

Novedad: la posibilidad de que el responsable audite al encargado para asegurarse de que está en condiciones de cumplir con la normativa.

Responsabilidad del responsable por elegir mal al encargado.

Delegado de Protección de Datos (DPO)

Figura obligatoria en varios supuestos:

- *Administración Pública.*
- *Empresas que realicen tratamientos a gran escala.*

Pero los EEMM pueden establecer supuestos adicionales.

El DPO será designado atendiendo a:

- *Sus cualidades profesionales.*
- *Conocimientos especializados en Derecho y en NNTT.*
- *Práctica en la protección de datos.*

Obligaciones del Responsable del Tratamiento

- ***Conservación Documentación***
- ***Implantar las Medidas de Seguridad***
- ***Realizar Análisis de Riesgos***
- ***Autorización o consulta previa a autorización de control***
- ***Designación DPO***
- ***Implantar mecanismos para verificar eficacia medidas de seguridad (auditores)***

Incidente de Seguridad

- ***Notificación violación de la seguridad de los datos a la autoridad de control***
  - Contenido: naturaleza, datos responsable, consecuencias, medidas adoptadas y documentar
- ***Comunicación al interesado:***
  - No necesario si: medidas de protección adecuadas adoptadas, esfuerzo desproporcionado o medidas posteriores para evitar materización riesgo.

Comentarios, cuestiones, sugerencias ,…

jlrivas@uvigo.es

http://webs.uvigo.es/jlrivas

@jlrivas