HACIA LA SEGURIDAD DE LOS DATOS DESPUES DEL REGLAMENTO EUROPEO

TOWARDS THE SECURITY DATA AFTER THE EUROPEAN REGULATION

Autores: José Luis Rivas López (jlrivas@uvigo.es)
Victor Salgado Seguín (v.salgado@udc.es)

Palabras clave: Reglamento UE 2016/679, Privacidad, responsable de fichero, análisis de riesgos

Keywords: EU Regulation 2016/679, Privacy, responsible for the file, risk analysis.

Resumen: En la actualidad, las universidades generan ingentes cantidades de datos que permiten obtener inteligencia aplicable a multitud de áreas del conocimiento académicas y científicas. Dichos datos se están almacenando en nubes públicas y privadas. Con el nuevo marco regulatorio aprobado recientemente por la Unión Europea conocido como Reglamento general de Protección de Datos (Reglamento UE 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016) y su futura aplicación a partir de mayo de 2018, explicaremos como afrontar el nuevos reto normativo y solventar las nuevas problemáticas ocasionadas.
Para ello, lo abordaremos desde el punto de vista técnico y legal. Alguno de puntos a tratar serán:

- Derechos de los interesados. En especial, el "derecho al olvido" y el derecho a la portabilidad de datos.
- El "Privacy by design".
- Medidas de seguridad flexibles y obligación de notificación del "Data breach".
- Consentimiento reforzado.
- Información ampliada al interesado.
- Evaluación de impacto en protección de datos y consulta previa.
- El Delegado de Protección de Datos (DPO).
- La nueva responsabilidad proactiva o "accountability"
- Los nuevos principios de la protección de datos de transparencia, minimización de datos y plazo de conservación.
- Códigos de conducta y certificación.
- Transferencia internacional de datos: el nuevo "Privacy Shield".
- Autoridades de control: competencias y coordinación.
- Sanciones, responsabilidad y recursos.

- Casos especiales y excepciones.
- Entrada en vigor y aplicación.
- Conclusiones.

Summary: currently, the universities generate enormous amounts of data that allow get intelligence applicable to crowd of areas of the knowledge academic and scientific. These data are being stored in public and private clouds. With the new regulatory framework recently approved by the European Union known as General Data Protection Regulation (EU Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016) and its future implementation from May 2018, we explain how to face the new regulatory challenge and solve new problems caused. To do this, we will take it from the technical and legal point of view. Some points to address will be:

- Rights of interested parties. In particular, the "right to oblivion" and the right to data portability.
- The "Privacy by design".
- Flexible security measures and notification obligation of the "Data breach".
- Reinforced consent.
- Applied information to interested.
- Assesment of impact on data protection and previous consultation.
- The Data Protection Officer (DPO).
- The new proactive responsibility or "accountability"
- The new principles of the protection of data of transparency, minimization of data and period of conservation.
- Codes of conduct and certification.
- International data transfer: the new "Privacy Shield".
- Control authorities: skills and coordination.
- Sanctions, responsibility and resources.
- Special cases and exceptions.
- Entry into force and application.
- Conclusions.

Un nuevo marco normativo

El pasado 4 de mayo de 2016 se publicó el largamente esperado nuevo Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos

y por el que se deroga la Directiva 95/46/CE. A dicha norma se la denomina Reglamento General de Protección de Datos y también por sus siglas "RGPD" o "GDPR", a nivel internacional. A efectos del presente artículo, la denominaremos simplemente como "el Reglamento".

Como su propio nombre indica, el Reglamento viene a derogar y sustituir la Directiva de 1995 y se aplicará por encima de toda la normativa europea y nacional aprobada en materia de protección de datos. A nivel jurídico, la diferencia fundamental entre una Directiva y un Reglamento es que, mientras la primera necesita de una legislación nacional que la "transponga" para su plena vigencia en los Estados Miembros, el Reglamento no requiere tal trámite y se aplica de forma directa.

Ello quiere decir, en el presente caso, que, aunque no se adopte ninguna legislación interna en la materia, el Reglamento será aplicable, en todos sus efectos, el día 25 de mayo de 2018. Marquemos, pues, bien esta fecha en el calendario.

¿Por qué una nueva regulación para la protección de datos?

Hay muchas razones para la necesidad de un nuevo marco normativo en materia de privacidad pero, sin duda, una de las más importantes es el gran cambio tecnológico y social que se produjo desde los años 90 hasta hoy en día. El desarrollo de Internet y el surgimiento de tecnologías como el omnipresente buscador Google, pasando por las redes sociales y llegando a las actuales plataformas de mensajería, han causado que las personas hayan cambiado radicalmente sus hábitos pasando de ser muy celosas de sus datos en los 90, donde sólo los facilitaban en contadas ocasiones y de forma controlada, hasta el escenario actual en el que se facilitan abiertamente dichos datos

Niveles de los datos

Dentro del Reglamento de Desarrollo de la LOPD (RD 1720/2007), existen tres niveles de seguridad distintos como son, el básico, el medio y el alto, que se indican en la siguiente figura.:

El nivel que hay que aplicar depende del tipo de datos que se almacenan en el fichero. Estas medidas de seguridad se aplican de forma acumulativa, es decir, de tal manera que el nivel alto debe cumplir también las medidas establecidas para los niveles medio y básico.

A partir del RGPD nos vamos a encontrar sólo con datos de carácter personal que además ha cambiado su definición. Un dato de persona es a partir de ahoral: toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;

Además, sólo nos encontraremos con categorías especiales de datos con prohibición de tratamiento salvo excepciones que son:

- Origen racial o étnico
- Opiniones políticas
- Creencias religiosas o filosóficas
- Pertenencias a sindicatos
- Tratamientos datos genéticos
- Biométricos (cualquier tipo de biometría)
- Datos de salud
- Orientación sexual

Es decir, desaparecen los 3 niveles de datos: bajo, medio y alto.

Responsabilidad proactiva o "accountability"

De todas sus grandes novedades, la más importante, sin duda, es la llamada "responsabilidad proactiva" o "accountability" en inglés. Básicamente, supone nuestra mayoría de edad en lo relativo a la protección de datos personales. Si la anterior Directiva y nuestra vigente Ley Orgánica 15/1999, de 13 de diciembre de 1999, de Protección de Datos de Carácter Personal (LOPD), nos llevaban de la mano al indicarnos los requisitos y obligaciones detalladas en el tratamiento de la información personal, el nuevo Reglamento deja más en nuestras manos el decidir qué medidas implantamos, pero, eso sí, debiendo justificar nuestra elección y, ante todo, acreditar documentalmente su cumplimiento.

Como dos ejemplos de ello, podemos poner la obligación de inscripción de ficheros y las medidas de seguridad:

1- Actualmente, la vigente LOPD en España dispone la necesidad de notificar a la Agencia Española de Protección de Datos todos aquéllos ficheros con datos de carácter personal que existan en nuestra organización. Por contra, el nuevo Reglamento nos exime de dicha

obligación, pero, eso sí, nos obliga a llevar internamente un "Registro de actividades de tratamiento" que deberemos poner a disposición de la Autoridad de Control por si nos fuere requerido.

2- En cuanto a las medidas de seguridad, el Titulo VIII de nuestro vigente Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento desarrollo de la Ley Orgánica 15/1999, de 13 de junio de protección de datos de carácter personal, regula tres niveles diferenciados, el básico, medio y el alto, en función del tipo de datos tratados y con medidas muy concretas para cada uno de estos niveles. El nuevo Reglamento, por su parte, nos dispensa de tal clasificación y medidas concretas, dejando, una vez más, en nuestras manos la fijación de las medidas concretas de seguridad que aplicamos sobre los datos pero debiendo, eso sí, justificar su pertinencia y probar su aplicación efectiva para cumplir los objetivos obligatorios de integridad y confidencialidad de la información personal.

Esto son sólo dos ejemplos, pero muy reveladores, respecto al cambio de paradigma en la normativa de protección de datos a partir de mayo de 2018.

Consentimiento e información reforzados

Dos de los pilares básicos de la normativa de protección de datos han sido siempre el consentimiento y la información:

1- El primero señala la regla general de que todo tratamiento de datos personales debe basarse en la previa autorización del interesado aunque, por supuesto, se admiten excepciones con base a la ley.

2- Por su parte, el segundo dispone que, con independencia de si necesito o no el consentimiento previo para el citado tratamiento, en todo caso tengo que informar a los interesados de la existencia del mismo así como de los elementos mínimos que nos pide la ley.

Pues bien, ambos pilares se ven enormemente reforzados en el nuevo Reglamento del siguiente modo:

1- En la LOPD actual, el consentimiento puede ser tácito, siempre que no se traten datos sensibles. Sin embargo, a partir de la aplicación del

Reglamento, el consentimiento deberá ser siempre expreso, sean cuales sean los datos tratados.

2- Respecto a la información, el nuevo Reglamento amplía enormemente el mínimo legal de la misma que hay que facilitar al interesado, incluyendo aspectos tales como el plazo durante el que vamos a tratar los datos, así como la identificación del Delegado de Protección de Datos o DPO, en su caso, o la existencia de decisiones automatizadas, entre otras muchas cuestiones.

Nuevos derechos del interesado

A los clásicos derechos de acceso, rectificación, cancelación y oposición (nuestros viejos "derechos ARCO"), se suman ahora otros como el famoso "derecho al olvido", que nos es otro que un derecho de cancelación actualizado, o el derecho a la limitación del tratamiento o el derecho a la portabilidad de datos.

Como mayor novedad, este último supone el derecho del interesado a recibir su información en un formato estructurado y de uso común, para su transmisión a otro responsable o, incluso, la obligación del anterior responsable de hacerlo directamente, aunque se trate de una empresa de la competencia. Será interesante ves su aplicación en servicios de cloud computing, por ejemplo.

Nuevos principios de la protección de datos y obligación de notificación del "data breach"

Respecto a los principios y aunque el nuevo Reglamento consolida los recogidos en la normativa anterior como el de finalidad, lealtad, calidad o seguridad de los datos, se crean algunos nuevos como el de transparencia, minimización y limitación del plazo de conservación:

1- Respecto a este último, ya nos referimos anteriormente a la hora de comentar las novedades de la información al interesado, donde hay que referirse expresamente a este punto. Este principio se refiere a la necesidad de limitar el plazo de tratamiento al estrictamente necesario con relación a la finalidad del mismo. Ni más ni menos.

2- Respecto al principio de transparencia, el Reglamento obliga a dar información clara, continua y ampliada al interesado tanto sobre el tratamiento de sus datos como sobre todas las vicisitudes e incidencias en el mismo. Buena muestra de ello es el deber de comunicar las violaciones de seguridad, tanto a la Autoridad de Control, en un plazo máximo de 72 horas, como a los propios interesados, si sus derechos se ven en riesgo.
3- En cuanto a la minimización (o "data minimization"), el Reglamento dispone la necesidad de reducir al máximo las categorías de datos tratados a los estrictamente necesarios para cada finalidad de tratamiento.

Herramientas de control interno reforzadas: Evaluación de impacto, DPO y "privacy by design"

Como comentábamos anteriormente, el nuevo Reglamento supone un cambio de paradigma en lo que suponen las obligaciones y el control de la protección de datos personales.

Así, se establece la obligación general de adoptar una política de "privacy by design" y de "privacy by default" en nuestra organización, de tal modo que, cada vez que vayamos a diseñar un nuevo producto, servicio o acción, debemos pensar en la privacidad de los usuarios desde el mismo principio, facilitando que, por defecto, sus datos estén debidamente protegidos sin que el interesado deba de hacer nada especial para ello.

Asimismo, cuando dichos nuevos proyectos vayan a implicar un riesgo especial para los derechos de los interesados, en supuestos específicos, el Reglamento obligará a realizar una Evaluación de impacto previa, en línea a lo exigido en otras normativas como la medioambiental o la de prevención de riesgos laborales, debiendo, en casos extremos, solicitar la autorización previa a la Autoridad de Control si el riesgo se concluye importante.

Paralelamente, surge la nueva figura del Delegado de Protección de Datos (conocido como "DPO" a nivel internacional), el cual deberá existir siempre en las AAPP, además de muchos otros ámbitos, y que funcionará como una suerte de asesor-controlador interno sobre el cumplimiento de la normativa de protección de datos, a la par que punto de contacto y garante para el interesado e intermediador con la Autoridad de Control. Dicho DPO podrá ser interno, integrado en la plantilla, o externo, como profesional freelance o asesor contratado.

Control externo y mecanismos de verificación de cumplimiento

Por su parte, el Reglamento mantiene las llamadas Autoridades de Control nacionales, como la Agencia Española de Protección de Datos en nuestro país, como garantes independientes del cumplimiento de esta normativa y coordinadas ahora bajo el paraguas del llamado "Comité" europeo que facilita su coordinación y coherencia a nivel internacional.
Dichas Autoridades conservan importantes competencias como las de inspección (actual auditoría) y, como no, las de sanción a presuntos infractores. Con relación a este último punto, el nuevo Reglamento sobresale por su potencial dureza en las multas administrativas las cuales, además de deber ser "efectivas, proporcionadas y disuasorias", podrán alcanzar los 10 millones de euros o el 2% del volumen de facturación o, en un nivel superior, hasta los 20 millones de euros o el 4% del volumen total de negocio (la cantidad que resulte mayor), poniendo en el ojo del huracán a las grandes compañías de telecomunicaciones y/o de Internet que no se veían muy afectadas potencialmente por el cuadro de sanciones anterior, aunque en el caso de España llegaran hasta los 600.000 euros potenciales.
Como mecanismos de verificación del cumplimiento, el nuevo Reglamento nos da la opción de confeccionar o adherirnos a códigos tipo específicos y/o sectoriales, así como de acudir a procesos de certificación "ad hoc" para demostrar tanto nuestra buena fe como nuestro grado de cumplimiento de la normativa en materia de

protección de datos, sin necesidad de elaboradas justificaciones y complicadas pruebas internas de verificación.

Transferencias internacionales de datos

Mención aparte merece la prolija regulación de las transferencias internacionales de datos que, como en la normativa anterior, sólo se permiten en casos contados cuando se garantice un nivel de protección de datos equivalente en el país de destino que el exigido en el territorio de la UE, admitiéndose contadas excepciones como las autorizaciones especiales, la adopción de normas corporativas vinculantes o el consentimiento explícito y consciente del interesado.

Sin duda, esta normativa está de máxima actualidad después de haberse anulado por Sentencia del Tribunal de Justicia de la Unión Europea (TJUE) en octubre de 2015 el llamado "Safe Harbour" o "Puerto Seguro" acordado entre la Comisión Europea y los EEUU y que permitían la transferencia de innumerables datos de europeos a las grandes compañías americanas con la mera formalización de su adhesión al mismo. Actualmente, el reciente "Privacy Shield" o "Escudo de Privacidad" que lo sustituye y que entró en vigor en agosto pasado, va a ser mirado con lupa tanto por las Autoridades de Control como por el propio TJUE a la luz del nuevo Reglamente en los próximos años.

Regulación nacional y sectorial

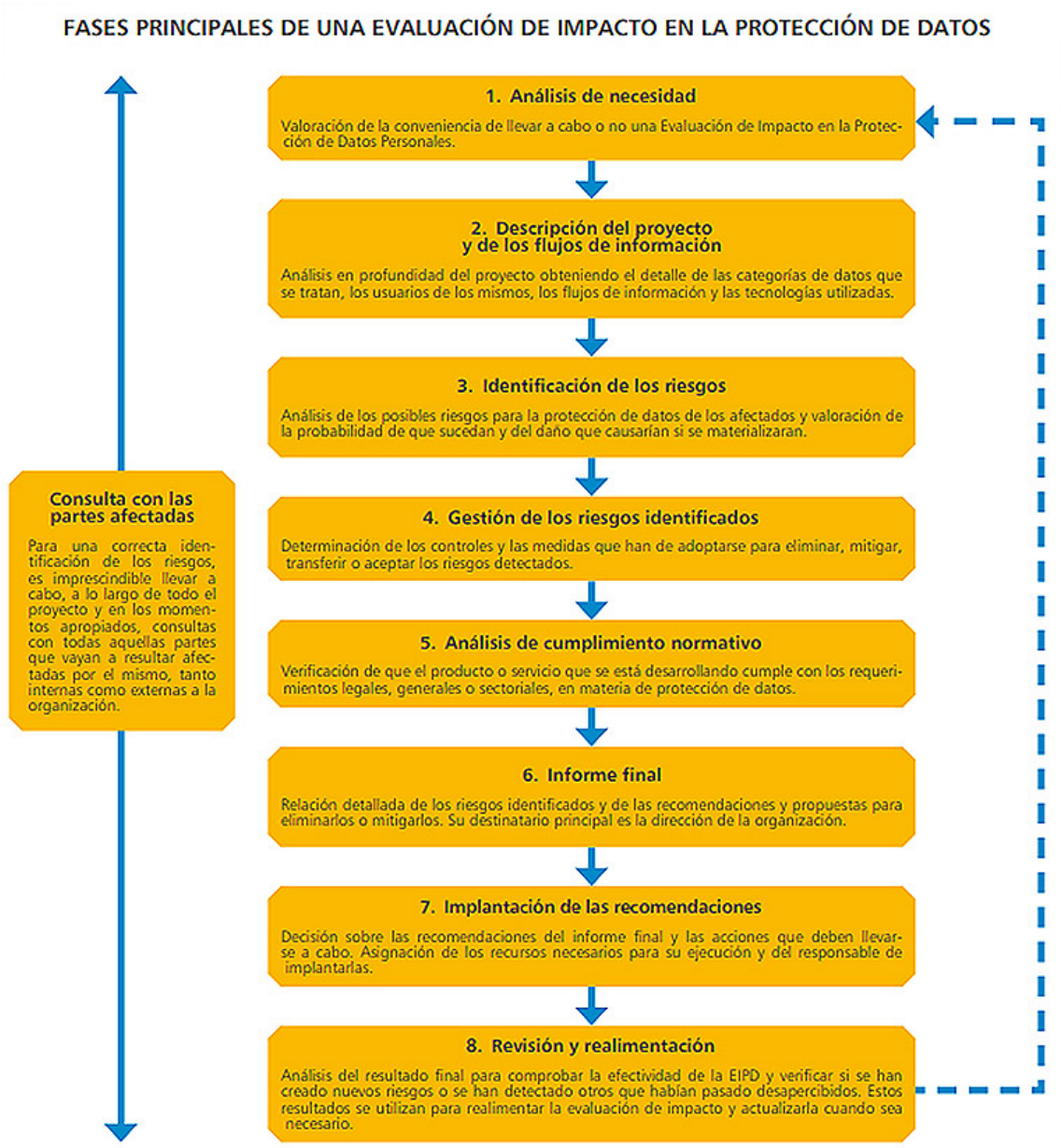
Aunque, como comentamos anteriormente, no sea necesario adoptar legislación interna para que el Reglamento sea directamente aplicable a partir del próximo 25 de mayo de 2018, otra cuestión es que no sea muy recomendable hacerlo, para garantizar una mayor coherencia y claridad de cumplimiento, así como, por otro lado, regular ámbitos sectoriales específicos que el propio Reglamento deja en manos de los Estados para regular "ad hoc" y fijar excepciones adicionales. Dichos ámbitos son los siguientes: Libertad de Expresión y de información, acceso a documentos oficiales, Número nacional de identificación, ámbito

laboral, archivo en interés público, investigación científica o histórica y fines estadísticos, obligaciones de secreto y regulación de iglesias y asociaciones religiosas. Todos estos ámbitos se podrán desarrollar normativamente por los Estados Miembros, con obligación de notificarlo a la Comisión Europea, antes del 25 de mayo de 2018.

Evaluación de impacto / análisis de Riegos

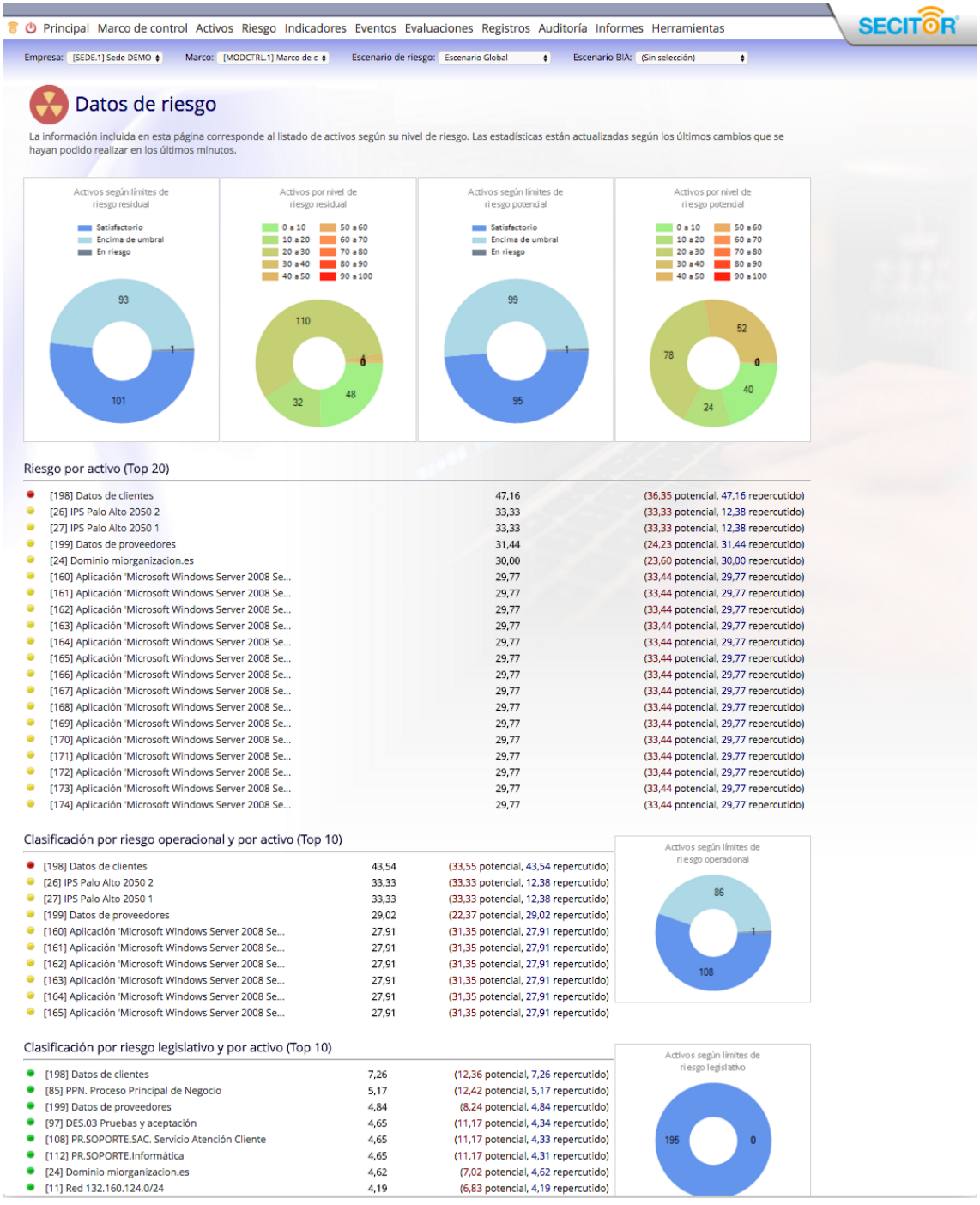
Uno de los puntos importantes del nuevo reglamento es la realización de análisis de riesgos en privacidad. Ya la AGPD en su guía para una evaluación de impacto en la protección de Datos Personales hace referencia a los dos grandes tipos de riesgos que nos vamos a enfrentar:

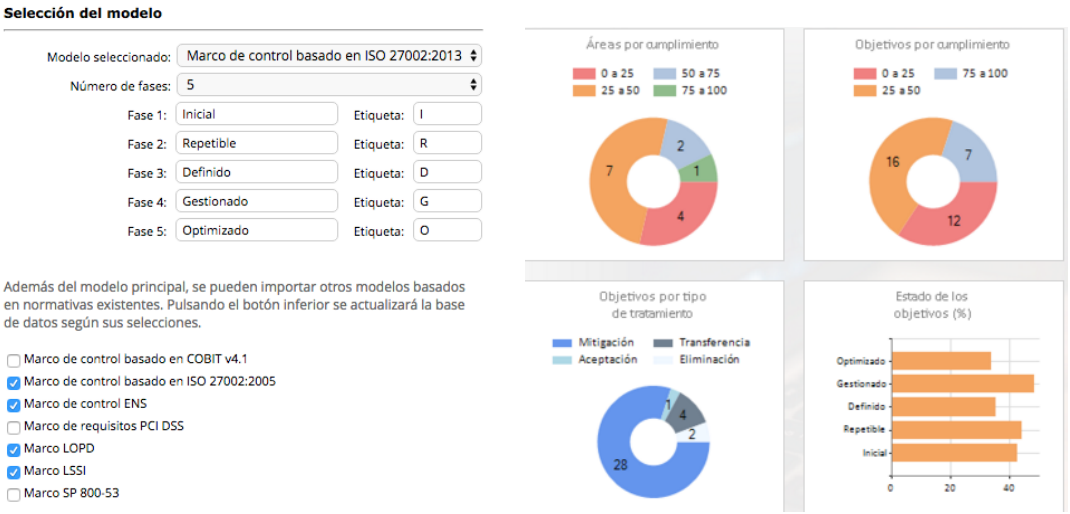
- El que afecta directamente a las personas
- El que afecta a la empresa/organismo



Una vez identificado los riesgos se trata de evitarlo o eliminarlo para ello hay que mitigarlo, transferirlo o aceptarlo.

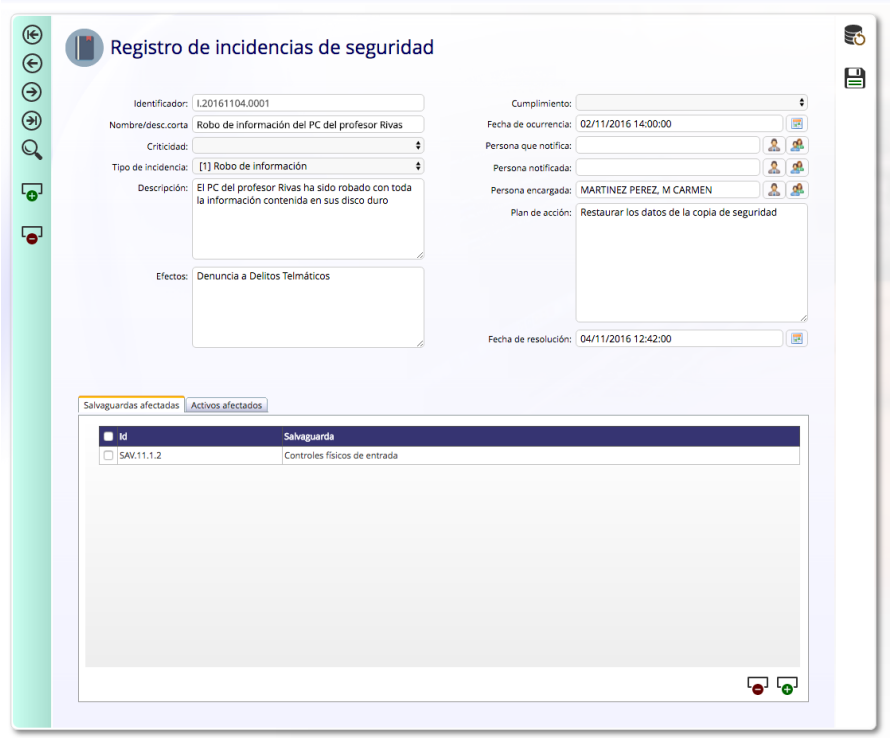
Como AAPP tenemos que realizar este tipo análisis de riesgos para el cumplimiento del Esquema Nacional de Seguridad (ENS) que junto con la Ley de Procedimiento Administrativo (LPAC) que ha entrado en vigor el mes pasado vamos a tener un análisis de riesgos con todos los activos, riesgos, salvaguardas de nuestra organización


Principal Marco de control Activos Riesgo Indicadores Eventos Evaluaciones Registros Auditoría Informes Herramientas
SECITOR
Empresa: [SEDE.1] Sede DEMO
Marco: [MODCTRL.1] Marco de c
Escenario de riesgo: Escenario Global
Escenario BIA: (Sin selección)
Datos de riesgo
La información incluida en esta página corresponde al listado de activos según su nivel de riesgo. Las estadísticas están actualizadas según los últimos cambios que se hayan podido realizar en los últimos minutos.
Activos según límites de riesgo residual
Satisfactorio
Encima de umbral
En riesgo
93
1
101
Activos por nivel de riesgo residual
0 a 10
10 a 20
20 a 30
30 a 40
40 a 50
50 a 60
60 a 70
70 a 80
80 a 90
90 a 100
110
0
32
48
Activos según límites de riesgo potencial
Satisfactorio
Encima de umbral
En riesgo
99
1
95
Activos por nivel de riesgo potencial
0 a 10
10 a 20
20 a 30
30 a 40
40 a 50
50 a 60
60 a 70
70 a 80
80 a 90
90 a 100
52
78
0
40
24
Riesgo por activo (Top 20)
[198] Datos de clientes 47,16 (36,35 potencial, 47,16 repercutido)
[26] IPS Palo Alto 2050 2 33,33 (33,33 potencial, 12,38 repercutido)
[27] IPS Palo Alto 2050 1 33,33 (33,33 potencial, 12,38 repercutido)
[199] Datos de proveedores 31,44 (24,23 potencial, 31,44 repercutido)
[24] Dominio miorganizacion.es 30,00 (23,60 potencial, 30,00 repercutido)
[160] Aplicación 'Microsoft Windows Server 2008 Se... 29,77 (33,44 potencial, 29,77 repercutido)
[161] Aplicación 'Microsoft Windows Server 2008 Se... 29,77 (33,44 potencial, 29,77 repercutido)
[162] Aplicación 'Microsoft Windows Server 2008 Se... 29,77 (33,44 potencial, 29,77 repercutido)
[163] Aplicación 'Microsoft Windows Server 2008 Se... 29,77 (33,44 potencial, 29,77 repercutido)
[164] Aplicación 'Microsoft Windows Server 2008 Se... 29,77 (33,44 potencial, 29,77 repercutido)
[165] Aplicación 'Microsoft Windows Server 2008 Se... 29,77 (33,44 potencial, 29,77 repercutido)
[166] Aplicación 'Microsoft Windows Server 2008 Se... 29,77 (33,44 potencial, 29,77 repercutido)
[167] Aplicación 'Microsoft Windows Server 2008 Se... 29,77 (33,44 potencial, 29,77 repercutido)
[168] Aplicación 'Microsoft Windows Server 2008 Se... 29,77 (33,44 potencial, 29,77 repercutido)
[169] Aplicación 'Microsoft Windows Server 2008 Se... 29,77 (33,44 potencial, 29,77 repercutido)
[170] Aplicación 'Microsoft Windows Server 2008 Se... 29,77 (33,44 potencial, 29,77 repercutido)
[171] Aplicación 'Microsoft Windows Server 2008 Se... 29,77 (33,44 potencial, 29,77 repercutido)
[172] Aplicación 'Microsoft Windows Server 2008 Se... 29,77 (33,44 potencial, 29,77 repercutido)
[173] Aplicación 'Microsoft Windows Server 2008 Se... 29,77 (33,44 potencial, 29,77 repercutido)
[174] Aplicación 'Microsoft Windows Server 2008 Se... 29,77 (33,44 potencial, 29,77 repercutido)
Clasificación por riesgo operacional y por activo (Top 10)
[198] Datos de clientes 43,54 (33,55 potencial, 43,54 repercutido)
[26] IPS Palo Alto 2050 2 33,33 (33,33 potencial, 12,38 repercutido)
[27] IPS Palo Alto 2050 1 33,33 (33,33 potencial, 12,38 repercutido)
[199] Datos de proveedores 29,02 (22,37 potencial, 29,02 repercutido)
[160] Aplicación 'Microsoft Windows Server 2008 Se... 27,91 (31,35 potencial, 27,91 repercutido)
[161] Aplicación 'Microsoft Windows Server 2008 Se... 27,91 (31,35 potencial, 27,91 repercutido)
[162] Aplicación 'Microsoft Windows Server 2008 Se... 27,91 (31,35 potencial, 27,91 repercutido)
[163] Aplicación 'Microsoft Windows Server 2008 Se... 27,91 (31,35 potencial, 27,91 repercutido)
[164] Aplicación 'Microsoft Windows Server 2008 Se... 27,91 (31,35 potencial, 27,91 repercutido)
[165] Aplicación 'Microsoft Windows Server 2008 Se... 27,91 (31,35 potencial, 27,91 repercutido)
Activos según límites de riesgo operacional
86
1
108
Clasificación por riesgo legislativo y por activo (Top 10)
[198] Datos de clientes 7,26 (12,36 potencial, 7,26 repercutido)
[85] PPN. Proceso Principal de Negocio 5,17 (12,42 potencial, 5,17 repercutido)
[199] Datos de proveedores 4,84 (8,24 potencial, 4,84 repercutido)
[97] DES.03 Pruebas y aceptación 4,65 (11,17 potencial, 4,34 repercutido)
[108] PR.SOPORTE.SAC. Servicio Atención Cliente 4,65 (11,17 potencial, 4,33 repercutido)
[112] PR.SOPORTE.Informática 4,65 (11,17 potencial, 4,31 repercutido)
[24] Dominio miorganizacion.es 4,62 (7,02 potencial, 4,62 repercutido)
[11] Red 132.160.124.0/24 4,19 (6,83 potencial, 4,19 repercutido)
Activos según límites de riesgo legislativo
195
0
Relaciones del activo
Riesgo
Vulnerabilidades
Salvaguardas
Amenazas
Protección de datos
Más...
Id. 219
Datos Expediente
Id. 126
Servicio de filtrado web
Id. 140
Servicio de pruebas IIS
Id. 37
Cluster FileNet
Id. 117
Servicio Antivirus
Id
Activo
[%]
126 Servicio de filtrado web 100
140 Servicio de pruebas IIS 100
37 Cluster FileNet 100
117 Servicio Antivirus 100



Incidentes de Seguridad

El Reglamento europeo obliga a notificar un incidente de seguridad (siempre que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales, etc.) a la autoridad de control en el plazo de 72 horas. Además, salvo excepciones también habrá que comunicar dichos incidentes de seguridad catalogados como violaciones al propio interesado.



Todo un reto por delante

Como hemos visto, tenemos un gran desafío por delante tanto para conocer como para desarrollar e integrar esta nueva normativa en nuestras organizaciones de cara a la entrada en aplicación del Reglamento el 25 de mayo de 2018.

La buena noticia es que aún tenemos tiempo, pero no debemos dormirnos en los laureles pues hay un enorme trabajo por delante que hacer para adaptarnos a este auténtico cambio de paradigma en la protección de este derecho fundamental que hemos venido en llamar privacidad.