Protección de datos y seguridad de la información

Ingrid González Hernández
Abogada

RESUMEN: La protección de datos y la seguridad de la información se han convertido en preocupaciones centrales en la era digital con importantes implicaciones legales para las organizaciones y los individuos. Las violaciones de la seguridad de los datos personales pueden tener consecuencias significativas para las organizaciones, como daños a la reputación, pérdidas financieras y responsabilidad legal. Por ello, es fundamental que las organizaciones cuenten con un sólido plan de respuesta ante las mismas, y apliquen en cumplimiento de la privacidad desde el diseño y por defecto, las medidas técnicas y organizativas adecuadas al riesgo o, en su caso, a la evaluación de impacto analizada, siempre sobre la base de cumplimiento de los principios de la protección de datos personales y la seguridad de la información.

Palabras clave: protección de datos, seguridad de la información, violación de seguridad, análisis de riesgos, evaluaciones de impacto.

ABSTRACT: Data protection and information security have become central concerns in the digital age with important legal implications for organisations and individuals. Breaches of personal data security can have significant consequences for organisations, such as reputational damage, financial loss and legal liability. It is therefore essential for organisations to have a robust breach response plan in place, and to implement privacy-compliant technical and organisational measures appropriate to the risk or, where appropriate, the impact assessment analysed, by design and by default, always on the basis of compliance with the principles of personal data protection and information security.

Keywords: data protection, information security, security breach, risk analysis, impact assessments.

LA INFORMACIÓN. 2.1 Definiciones y distinciones. 2.2 Acuerdo de Encargo de Tratamiento. 2.3 Medidas para la contratación pública. 2.3.1 Vertiente Legal: Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones. 2.3.2 Vertiente Técnica: Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. 3. PRIVACIDAD DESDE EL DISEÑO Y POR DEFECTO. PRINCIPIOS FUNDAMENTALES. 4. EL ANÁLISIS DE RIESGOS EN PROTECCIÓN DE DATOS. 5. EVALUACIÓN DE IMPACTO EN PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL. 6. SEGURIDAD DE LOS DATOS PERSONALES: APLICACIÓN DE MEDIDAS TÉCNICAS Y ORGANIZATIVAS APROPIADAS. 7. NOTIFICACIONES DE VIOLACIONES DE SEGURIDAD

1. INTRODUCCIÓN A LA PROTECCIÓN DE DATOS Y SEGURIDAD DE LA INFORMACIÓN EN LA ERA DIGITAL: UNA PERSPECTIVA LEGAL

1.1. La importancia de la protección de datos y la seguridad de la información

La dependencia global hacia la tecnología ha llevado a una cantidad sin precedentes de datos que se generan, procesan y almacenan todos los días. Estos datos a menudo incluyen información personal y confidencial, que, si se maneja mal o se accede a ella sin autorización, podría tener graves consecuencias para los individuos y las organizaciones.

El crecimiento y valor exponencial de los datos, combinado con la ubicuidad de los dispositivos conectados a internet, ha creado nuevas oportunidades para que los actores maliciosos exploren las vulnerabilidades de seguridad y protección de la información, con el fin de obtener acceso no autorizado a esa fuente de valor denominado: dato.

Es por ello por lo que, la protección de datos y la seguridad de la información se han convertido en preocupaciones primordiales. Las violaciones de datos y los ciberataques ya no son incidentes aislados, son amenazas generalizadas.

Es esencial comprender la importancia de la protección de datos y la seguridad de la información en esta era digital, así como los posibles riesgos y consecuencias que pueden surgir de las violaciones de datos, los ataques cibernéticos y el acceso no autorizado. Y es que, la materialización de estos eventos puede traducirse en (i) pérdidas financieras significativas, como pudieran ser los gastos relacionados con la respuesta a incidentes, honorarios legales, así como los costes asociados con la implementación de medidas correctivas; (ii) daños reputacionales de calado que conducen a una pérdida de confianza entre los ciudadanos/clientes, o cualquier otro tercero afectado/interesado; (iii) interrupciones operativas en los sistemas e infraestructuras críticos, lo que lleva a un tiempo de inactividad operativo y pérdida de productividad e, incluso, (iv) sanciones

legales por incumplimiento de las regulaciones y normativas de protección de datos de carácter personal.

1.2. Principios jurídicos de la protección de datos de carácter personal y la seguridad de la información

A medida que el panorama digital ha ido evolucionando, también lo ha hecho el marco regulatorio que rige la protección de datos y la seguridad de la información con el fin de abordar estos desafíos emergentes.

Claro ejemplo de ello lo vemos en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 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 (en adelante, Reglamento General de Protección de Datos o RGPD) diseñado no sólo para proteger los derechos de privacidad de las personas, sino también para fomentar una cultura de responsabilidad y transparencia entre las organizaciones que manejan datos personales. De ahí que uno de los objetivos fundamentales del Reglamento General de Protección de Datos fuera el de armonizar las leyes de protección de datos en todos los estados miembros de la Unión Europea creando un marco normativo común que ayudara a fortalecer el derecho a la privacidad y la protección de datos de los residentes de la Unión Europea.

El RGPD apoya sus cimientos en siete principios relativos al tratamiento de datos personales y exige que todo tratamiento se ajuste a ellos:

- **Licitud, lealtad y transparencia:** Los datos personales deben tratarse de forma lícita, justa y transparente. Esto significa que el tratamiento de datos debe tener una base jurídica legítima, no debe ser discriminatorio y los interesados deben ser informados sobre el tratamiento de sus datos.
- **Limitación de la finalidad**: Los datos personales deben recogerse con fines determinados, explícitos y legítimos, y no deben tratarse posteriormente de manera incompatible con dichos fines.
- **Minimización de los datos:** Los datos personales deben ser adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que se tratan. Esto significa que las organizaciones sólo deben recopilar y tratar la cantidad mínima de datos personales necesarios para el fin especificado.
- **Exactitud:** Los datos personales deben ser exactos y, cuando sea necesario, mantenerse actualizados. Esto significa que las organizaciones deben tomar medidas razonables para garantizar que los datos personales son exactos y, cuando sea necesario, rectificar o suprimir los datos inexactos.
- **Limitación del plazo de conservación:** Los datos personales deben conservarse en una forma que permita la identificación de los interesados du-

rante un periodo no superior al necesario para los fines para los que se tratan los datos personales. Esto significa que las organizaciones deben tener una política de conservación y supresión de la información que garantice que los datos personales no se conservan más tiempo del necesario.

- **Integridad y confidencialidad:** Los datos personales deben tratarse de forma que se garantice una seguridad adecuada, incluida la protección contra el tratamiento no autorizado o ilícito y contra la pérdida, destrucción o daño accidentales. Esto significa que las organizaciones deben aplicar medidas técnicas y organizativas para proteger los datos personales.
- **Responsabilidad proactiva:** No sólo se debe cumplir, sino tener la capacidad para demostrar que se ha cumplido.

1.3. Aplicación extraterritorial y transferencias transfronterizas de datos

Si bien lo anterior, el alcance del RGPD va más allá de las fronteras de la UE al ser aplicable, no solo a las organizaciones con sede en la UE, sino también a aquellas ubicadas fuera de la UE que traten datos personales de residentes de la UE en relación con la oferta de bienes o servicios o con el control de su comportamiento.

Llegados a este punto, y entendiendo que nos encontramos en un mundo absolutamente conectado, es importante tener en cuenta que el RGPD también regula las transferencias internacionales de datos, que son las transferencias de datos que se producen desde el Espacio Económico Europeo (EEE) a países fuera del EEE. El RGPD exige que dichas transferencias cumplan determinadas salvaguardias para garantizar la protección de los datos personales, entre ellos:

- **Transferencias basadas en una decisión de adecuación**: La Comisión Europea puede determinar que un tercer país garantiza un nivel adecuado de protección de datos y, por lo tanto, los datos personales pueden transferirse libremente a ese país sin más salvaguardias[1].

---

[1] Cuando las entidades receptoras de los datos se encuentren en un país, un territorio o uno o varios sectores específicos de ese país u organización internacional que hayan sido declarados de nivel de protección adecuado por la Comisión Europea. Hasta la fecha los países y territorios están declarados como adecuados: Suiza. Decisión 2000/518/CE de la Comisión, de 26 de julio de 2000; Canadá. Decisión 2002/2/CE de la Comisión, de 20 de diciembre de 2001, respecto de las entidades sujetas al ámbito de aplicación de la ley canadiense de protección de datos; Argentina. Decisión 2003/490/CE de la Comisión, de 3 de junio de 2003; Guernsey. Decisión 2003/821/CE de la Comisión, de 21 de noviembre de 2003; Isla de Man. Decisión 2004/411/CE de la Comisión, de 28 de abril de 2004; Jersey. Decisión 2008/393/CE de la Comisión, de 8 de mayo 2008; Islas Feroe. Decisión 2010/146/UE de la Comisión, de 5 de marzo de 2010; Andorra. Decisión 2010/625/UE de la Comisión, de 19 de octubre de 2010; Israel. Decisión 2011/61/UE de la Comisión, de 31 de enero de 2011; Uruguay. Decisión 2012/484/UE, de la Comisión,

- **Transferencias basadas en garantías adecuadas** sin que requieran ninguna autorización expresa de una autoridad de control, como:
  - — Un instrumento jurídicamente vinculante y exigible entre las autoridades u organismos públicos.
  - — Normas Corporativas Vinculantes: Las organizaciones multinacionales pueden adoptar normas corporativas vinculantes (BCR), que son un conjunto de normas internas para las transferencias internacionales de datos dentro del grupo de empresas. Las BCR deben ser aprobadas por una autoridad supervisora y proporcionar un nivel suficiente de protección de los datos personales.
  - — Cláusulas contractuales tipo: El RGPD permite el uso de cláusulas contractuales tipo (CCT) entre responsables o encargados del tratamiento de datos en la UE y responsables o encargados del tratamiento de datos fuera de la UE. Las CCT son plantillas preaprobadas para contratos que incluyen determinadas salvaguardias para garantizar la protección de los datos personales durante las transferencias internacionales[2].
  - — Códigos de conducta y certificación: El GDPR también permite el desarrollo de códigos de conducta y mecanismos de certificación para las transferencias internacionales de datos. Estos códigos de conducta y mecanismos de certificación deben ser aprobados por una autoridad de control y deben garantizar un nivel suficiente de protección de los datos personales.
- **Transferencias basadas en excepciones para situaciones específicas**. Estas excepciones incluyen:
  - — Consentimiento explícito: Los datos personales pueden transferirse fuera del EEE si el interesado ha dado su consentimiento explícito a la transferencia
  - — Ejecución de un contrato: La transferencia es necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento, o entre el responsable del tratamiento y otra persona física o jurídica, pero en interés del interesado.
  - — Interés público: Los datos personales pueden transferirse fuera del EEE si la transferencia es necesaria por razones de interés público, como la investigación científica o histórica.

---

de 21 de agosto de 2012; Nueva Zelanda. Decisión 2013/65/UE de la Comisión, de 19 de diciembre de 2012; Japón. Decisión de 23 de enero de 2019; Reino Unido. Decisión de 28 de junio de 2021; República de Corea. Decisión de 17 de diciembre de 2021.

[2] Decisión de Ejecución (UE) 2021/914 DE LA COMISIÓN de 4 de junio de 2021 relativa a las cláusulas contractuales tipo para la transferencia de datos personales a terceros países de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo

— Necesarios para reclamaciones legales: Los datos personales pueden transferirse fuera del EEE si la transferencia es necesaria para el establecimiento, ejercicio o defensa de reclamaciones legales.
— Intereses vitales: Los datos personales pueden transferirse fuera del EEE si la transferencia es necesaria para proteger los intereses vitales del interesado cuando esté física o jurídicamente incapacitado para dar su consentimiento.
— Registro público: La transferencia se realice desde un registro público que, tenga por objeto facilitar información al público y esté abierto a la consulta del público en general o de cualquier persona que pueda acreditar un interés legítimo, pero sólo en la medida en que se cumplan las condiciones que establece el Derecho de la Unión o de los Estados miembros para la consulta.

Es importante señalar que estas excepciones deben interpretarse de forma restrictiva y aplicarse únicamente en circunstancias específicas, y que el RGPD exige a los responsables y encargados del tratamiento que documenten y justifiquen el uso de dichas excepciones.

1.4. Marco jurídico local y sectorial

Cuando se adopta un Reglamento europeo, es directamente aplicable y vinculante en todos los Estados miembros de la UE, por lo que no es necesaria su transposición nacional al ordenamiento jurídico de cada Estado miembro. Esto significa que el Reglamento pasa automáticamente a formar parte del ordenamiento jurídico nacional y debe ser aplicado y ejecutado por las autoridades nacionales.

Sin detrimento de lo anterior, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y Garantía de los Derechos Digitales (en adelante, LOPDGDD) fue aprobada por el Parlamento español en diciembre de 2018 y entró en vigor el 6 de diciembre de 2018.

La LOPDGDD sustituye a la anterior ley española de protección de datos, promulgada en 1999, y adapta la legislación española al Reglamento General de Protección de Datos. La LOPDGDD, siguiendo las directrices del RGPD refuerza los derechos de las personas en relación con el tratamiento de sus datos personales e impone mayores obligaciones a los responsables y encargados del tratamiento. También, de forma adicional al RGPD, incluye disposiciones sobre derechos digitales, como el derecho a la neutralidad de Internet, el derecho a la educación digital y el derecho a la desconexión digital.

En lo que a la seguridad de la información se refiere, la LOPDGDD introduce un aspecto sumamente importante en su Disposición adicional primera, sobre las medidas de seguridad en el ámbito del sector público, señalando que: *1. El Esquema Nacional de Seguridad incluirá las medidas que deban implantarse en caso de tratamiento de datos personales para evitar su pérdida, alteración o acceso no autoriza-*

do, adaptando los criterios de determinación del riesgo en el tratamiento de los datos a lo establecido en el artículo 32 del Reglamento (UE) 2016/679. 2. Los responsables enumerados en el artículo 77.1 de esta ley orgánica deberán aplicar a los tratamientos de datos personales las medidas de seguridad que correspondan de las previstas en el Esquema Nacional de Seguridad, así como impulsar un grado de implementación de medidas equivalentes en las empresas o fundaciones vinculadas a los mismos sujetas al Derecho privado. En los casos en los que un tercero preste un servicio en régimen de concesión, encomienda de gestión o contrato, las medidas de seguridad se corresponderán con las de la Administración pública de origen y se ajustarán al Esquema Nacional de Seguridad. Ello deja claro que, aunque la LOPDGDD y Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS) son dos marcos legales diferentes que tienen objetivos distintos, operan de forma complementaria en el sentido de que ambos pretenden garantizar la protección de los datos personales y los sistemas de información en España.

El ENS, se configura como un conjunto de medidas técnicas y organizativas destinadas a garantizar la seguridad de los sistemas de información utilizados por la Administración Pública española, incluyendo directrices para la gestión de riesgos, el control de accesos y la gestión de incidentes. El ENS tiene por objeto asegurar el acceso, la confidencialidad, la integridad, la trazabilidad, la autenticidad, la disponibilidad y la conservación de los datos, la información y los servicios utilizados por las entidades públicas.

Con todo, cuando hablemos de seguridad de la información en el sector público, tenemos que llevar de la mano a ambas normas. El cumplimiento de ambos marcos es obligatorio para todas las entidades públicas en España y constituye un paso importante para garantizar la protección de los datos personales y los sistemas de información.

2. RESPONSABILIDADES DEL RESPONSABLE DEL TRATAMIENTO Y DEL ENCARGADO DEL TRATAMIENTO EN LA SEGURIDAD DE LA INFORMACIÓN

2.1. Definiciones y distinciones

Con carácter previo a definir y determinar las responsabilidades tanto del responsable como del encargado del tratamiento en la seguridad de la información es esencial definir cada una de estas figuras, conforme al RGPD:

- «**responsable del tratamiento**»: es la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, **determine los fines y medios del tratamiento**; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros.

- **«encargado del tratamiento»:** es la persona física o jurídica, autoridad pública, servicio u otro organismo que **trate datos personales por cuenta del responsable del tratamiento3.**

Por tanto, un responsable del tratamiento es una entidad que determina los fines y medios del tratamiento de los datos personales que están bajo su responsabilidad. Esto significa que decide qué datos se tratan, por qué y para qué se tratan. Los responsables del tratamiento pueden ser empresas, organizaciones o agencias gubernamentales que recogen datos personales directamente de las personas, por ejemplo, cuando se suscriben a un servicio o realizan una compra. Según la legislación de protección de datos, los responsables del tratamiento tienen varias responsabilidades que deben cumplir, entre las que se incluyen:

- Tratar los datos personales de forma lícita, justa y transparente. Deben tener una base jurídica para el tratamiento de datos personales y proporcionar información clara a los interesados sobre las actividades de tratamiento.
- Recopilar y tratar los datos personales únicamente con fines específicos, explícitos y legítimos.
- Garantizar que los datos personales que tratan son adecuados, pertinentes y limitados a lo necesario para los fines para los que se tratan.
- Garantizar que los datos personales son exactos y se mantienen actualizados.
- Conservar los datos personales únicamente el tiempo necesario para los fines para los que se tratan.
- Mantener registros de sus actividades de tratamiento y ponerlos a disposición de las autoridades de control que lo soliciten.
- Aplicar medidas técnicas y organizativas adecuadas para garantizar la seguridad de los datos personales.
- Realizar una Evaluación de Impacto en Protección de Datos (en adelante, EIPD) cuando sea probable que las actividades de tratamiento entrañen un alto riesgo para los derechos y libertades de los interesados.
- Aplicar medidas de protección de datos desde el principio del diseño de sus actividades de tratamiento y garantizar que la configuración de privacidad se establece por defecto.
- Nombrar a un Delegado de Protección de Datos (en adelante, DPD) cuando resulte obligatorio o de forma voluntaria en pro de su responsabilidad proactiva.

---

3 Guía "El encargado del tratamiento en el Reglamento General de Protección de Datos (RGPD)" de la Autoridad Catalana de Protección de Datos: <https://apdcat.gencat.cat/web/.content/03-documentacio/Reglament_general_de_proteccio_de_dades/documents/Guia-encargado-del-tratamiento-RGPD-CAST.pdf>

- Cooperar con las autoridades de control, como las autoridades de protección de datos, y proporcionarles la información que necesiten para garantizar el cumplimiento de la normativa aplicable en esta materia.

Además de los responsables del tratamiento, los encargados del tratamiento también desempeñan un papel importante en la protección de datos. Un encargado del tratamiento es una entidad que trata datos personales en nombre y por cuenta del responsable del tratamiento. Puede tratarse de empresas que prestan servicios informáticos, de gestión o control, para cuyo cumplimiento requieren el tratamiento de datos de carácter personal que están bajo el control del responsable del tratamiento. Los encargados del tratamiento no tienen control sobre los datos personales y sólo deben tratarlos siguiendo las instrucciones del responsable del tratamiento.

En virtud de la legislación sobre protección de datos, concretamente el artículo 28 del RGPD, determina cómo debe configurarse esta relación responsable-encargado, indicando entre otras cuestiones que, los encargados del tratamiento deben tratar los datos personales únicamente siguiendo las instrucciones del responsable del tratamiento, además, deben tomar las medidas de seguridad apropiadas para proteger los datos personales contra el tratamiento no autorizado o ilegal, la pérdida accidental, la destrucción o el daño, así como, en caso de contratar a subencargados del tratamiento, sólo podrán hacerlo con aquellos que ofrezcan garantías suficientes para aplicar las medidas técnicas y organizativas apropiadas para garantizar la seguridad del tratamiento

Del mismo modo, deben asistir al responsable del tratamiento en el cumplimiento de algunas obligaciones que le son propias como la de dar respuesta a las solicitudes de los interesados para ejercer sus derechos en virtud del RGPD o, la de realizar evaluaciones de impacto sobre la protección de datos y la consulta a las autoridades de control.

Una vez finalizada la relación entre las partes, los encargados del tratamiento deberán suprimir o devolver todos los datos personales al responsable del tratamiento al término de la prestación de los servicios, a menos que la ley les obligue a conservarlos.

Con todo, es claro que tanto los responsables como los encargados del tratamiento son responsables de garantizar la seguridad y privacidad de los datos personales. Si bien, todas estas obligaciones no sólo forman máximas legales incluidas en el RGPD y la LOPDGDD, sino que la norma obliga a que consten por escrito en un Acuerdo de Encargo de Tratamiento.

2.2. Acuerdo de Encargo de Tratamiento

A medida que las organizaciones dependen cada vez más de proveedores externos para el suministro de bienes y servicios, la gestión de los riesgos asociados a estas relaciones se ha vuelto más crítica. Cuando se trata de protección de

datos y seguridad de la información, estos riesgos pueden ser significativos. Por lo tanto, la gestión de riesgos de proveedores y terceros se ha convertido en una parte crítica del marco de gestión de riesgos de cualquier organización.

Para gestionar eficazmente los riesgos de proveedores —*encargados del tratamiento*— y las organizaciones deben llevar a cabo una diligencia debida y evaluaciones de riesgos antes de contratarlos. Este proceso incluye:

- Comprobación de los antecedentes del proveedor. Los responsables del tratamiento deben revisar los antecedentes del proveedor, incluyendo su historia, reputación y experiencia en la prestación de servicios similares. Esto puede ayudar a identificar cualquier señal de alarma que pueda indicar riesgos potenciales.
- Evaluar las políticas y procedimientos de protección de datos y seguridad de la información del proveedor. Los responsables del tratamiento deben revisar las políticas y procedimientos de protección de datos y seguridad de la información del proveedor para asegurarse de que cumplen las normas de la organización y las leyes y reglamentos pertinentes.
- Evaluación de las medidas de seguridad técnicas y organizativas del proveedor. Los responsables del tratamiento deben revisar las medidas de seguridad técnicas y organizativas del proveedor para asegurarse de que son adecuadas y eficaces.
- Realizar una evaluación de riesgos. Los responsables del tratamiento deben llevar a cabo una evaluación de riesgos para identificar cualquier riesgo potencial asociado con los servicios o productos del proveedor.

Todo ello se debe recoger de forma expresa en un contrato entre las partes que se ha venido denominando Acuerdo de Encargo de Tratamiento[4], en el que, además de indicarse las obligaciones que tiene el responsable del tratamiento con respecto a los datos e información que va a facilitar al encargado del tratamiento, también opera como una máxima de cumplimiento para el encargado, en tanto se deben recoger las directrices básicas sobre qué se le permite hacer con los datos y que no.

En el sector público la regulación con respecto a la relación responsable-encargado y la seguridad de la información ha venido pivotando, además de —*como resulta obvio*— por el RGPD y la LOPDGDD, con carácter particular por:

- Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones (RD-Ley 14/2019) por las modificaciones introducidas en la Ley 9/2017, de 8 de

---

[4] Directrices para la elaboración de contratos entre responsables y encargados del tratamiento de la Agencia Española de Protección de Datos: <https://www.aepd.es/es/documento/guia-directrices-contratos.pdf#:~:text=El%20RGPD%20exige%20la%20autorizaci%C3%B3n,por%20parte%20de%20un%20tercero>

noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS)

2.3. Medidas para la contratación pública

2.3.1. Vertiente Legal: Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones.

En lo que respecta al RD-Ley 14/2019, en su capítulo III (artículo 5) vino a regular varias medidas en materia de contratación pública. Concretamente, modificó varios artículos de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014 (en adelante, Ley 9/2017), con la finalidad de introducir medidas que garantizaran en todas las fases de la contratación (expediente de contratación, licitación y ejecución del contrato) el respeto por parte de contratistas y subcontratistas de la legislación de la Unión Europea en materia de protección de datos. ¿Qué implicación práctica tienen estas modificaciones?

En primer lugar, el RD-Ley 14/2019 modificó el artículo 35 *(Contenido mínimo del contrato),* para incluir, como **contenido mínimo de los contratos, la referencia expresa al sometimiento por parte del contratista a la normativa nacional y de la Unión Europea en materia de protección de datos.** Lo que implica que, las entidades públicas deben incluir en los contratos de forma expresa las referencias al Reglamento General Europeo de Protección de Datos, así como, a la LOPDGDD.

En segundo lugar, y por lo que **respecta al régimen de invalidez de los contratos**, se añade un subapartado al artículo 39.2, para incluir, **como causa de nulidad de pleno derecho, la celebración de contratos por parte de poderes adjudicadores que omitan mencionar en los pliegos las obligaciones del futuro contratista en materia de protección de datos** a los que se refiere el nuevo artículo 122.2 de la Ley 9/2017, en la redacción dada a dicho precepto por el RD-Ley 14/2019. La aplicación de la consecuencia jurídica máxima que contempla el ordenamiento jurídico, esto es, de la nulidad de pleno Derecho, se ha considerado adecuada dada la importancia que en determinados casos puede presentar para los intereses de la seguridad nacional conocer la ubicación de los servidores en los que se alojarán los datos que ceda la Administración con motivo de la ejecución de un contrato público, desde dónde se van a prestar los

servicios asociados a los mismos y asegurar el sometimiento de la ejecución de ese contrato a la normativa nacional y de la Unión Europea en materia de protección de datos. Es importante tener en consideración que, según la redacción de este artículo las obligaciones del contratista en materia de protección de datos que se establecen en el nuevo artículo 122.2 deben estar recogidas desde el pliego.

En tercer lugar, y en el contexto de la regulación de los requisitos para contratar con el sector público, se modificó el artículo 71.2.d) de la Ley 9/2017, para incluir, como **circunstancia que impedirá a los empresarios contratar** con las entidades comprendidas en el artículo 3 de dicha Ley, **el haber dado lugar a la resolución firme de cualquier contrato celebrado con una de tales entidades por incumplimiento culpable de las obligaciones que los pliegos hubieren calificado como esenciales** de acuerdo con lo previsto en el art. 211.1.f) de la propia Ley. De conformidad con la nueva redacción del artículo 122.2, las obligaciones incluidas en el mismo (122.2 letras a) a e) de la Ley 9/2017) **deben ser calificadas como esenciales a los efectos de lo previsto en el artículo 211.1.f), lo que implicaría que es una causa de resolución del contrato por el incumplimiento de una obligación principal del mismo.**

En cuarto lugar, se dio una nueva redacción al artículo 116.1 de la Ley 9/2017, introduciendo un segundo párrafo relativo **al expediente de contratación de los contratos cuya ejecución requiera de la cesión de datos** —*que no es lo mismo que un encargo de tratamiento*— por parte de entidades del sector público al contratista. En virtud de esta modificación, **se incluye la obligación del órgano de contratación de especificar en el expediente cuál será la finalidad de los datos que vayan a ser cedidos.** Esta nueva redacción va de la mano con la nueva redacción del artículo 202.1 de la Ley 9/2017, en tanto viene a indicar que, **cuando se produzca tal comunicación de datos, se debe indicar en el anuncio de licitación y en los pliegos las condiciones recogidas en el artículo 202.1.**

En quinto lugar, y como se ha indicado previamente, se dio una nueva redacción al artículo 122.2 de la Ley 9/2017, **relativo a los pliegos de cláusulas administrativas particulares**. En concreto:

- se añade un párrafo tercero a este apartado para **incluir la obligación de los pliegos de mencionar expresamente** la obligación del futuro contratista de respetar la normativa vigente en **materia de protección de datos.**
- Asimismo, se añadió un párrafo cuarto relativo a los contratos que exijan el tratamiento por el contratista de datos personales por parte del responsable del tratamiento, indicando que en estos casos será obligatorio hacer constar en el pliego tanto la finalidad de la cesión de datos como la obligación de la empresa adjudicataria de mantener al contratante al corriente de la ubicación de los correspondientes servidores.

- También se añade un párrafo quinto para establecer que los extremos mencionados en el párrafo cuarto deben hacerse constar en los **pliegos como obligaciones esenciales a los efectos del régimen de resolución del contrato.**

Llama la atención que, el legislador parece diferenciar las exigencias del artículo 28 del Reglamento General Europeo de Protección de Datos a las exigencias reguladas en las letras a) a e) de la nueva redacción del artículo 122.2 de la Ley 9/2017, señalando que *sin perjuicio de lo establecido en el artículo 28.2 del Reglamento*, en los contratos en los que el contratista requiera el tratamiento de datos por cuenta de la entidad como responsable del tratamiento, en el pliego se hará constar:

- La finalidad para la cual se cederán dichos datos.
- La obligación del futuro contratista de someterse en todo caso a la normativa protectora de datos de carácter personal
- La obligación de la empresa adjudicataria de presentar antes de la formalización del contrato una declaración en la que ponga de manifiesto dónde van a estar ubicados los servidores y desde dónde se van a prestar los servicios asociados a los mismos.
- La obligación de comunicar cualquier cambio que se produzca, a lo largo de la vida del contrato, de la información facilitada en la declaración a que se refiere el punto anterior.
- La obligación de los licitadores de indicar en su oferta, si tienen previsto subcontratar los servidores o los servicios asociados a los mismos, el nombre o el perfil empresarial, definido por referencia a las condiciones de solvencia profesional o técnica, de los subcontratistas a los que se vaya a encomendar su realización.

En sexto lugar, el RD-Ley 14/2019 da una nueva redacción al artículo 202.1 de la Ley 9/2017, regulador de las condiciones especiales de ejecución del contrato de carácter social, ético, medioambiental o de otro orden. En concreto, se introduce un párrafo tercero relativo a **los pliegos correspondientes a contratos cuya ejecución implique la cesión de datos por las entidades del sector público al contratista.** Mediante esta adición se impone la exigencia de que los **pliegos incluyan, como condición especial de ejecución, la obligación del contratista de someterse a la normativa nacional y de la Unión Europea en materia de protección de datos**. Asimismo, en los pliegos debe advertirse al contratista de que esta obligación **tiene el carácter de obligación contractual esencial a los efectos del régimen de resolución del contrato.**

En séptimo lugar, el RD-Ley da una nueva redacción al artículo 215.4 de la Ley 9/2017, relativo a la subcontratación, para incluir, **entre las obligaciones del contratista principal, la de asumir la total responsabilidad de la ejecución del contrato frente a la Administración también por lo que respecta a la obligación de sometimiento a la normativa nacional y de la Unión Euro-**

pea en materia de protección de datos. Viene a reconocer de forma expresa lo indicado en los artículos 28.2, y más concretamente, en el 28.4 del Reglamento General Europeo de Protección de Datos.

2.3.2. Vertiente Técnica: Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad

El pasado 5 de mayo de 2022 entró en vigor del Real Decreto 311/2022, de 3 de mayo de 2022, por el que se regula el Esquema Nacional de Seguridad. El principal objetivo del Esquema Nacional de Seguridad (ENS) es crear las condiciones necesarias de seguridad en el uso de los medios electrónicos, a través de medidas que puedan garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos, y que permitan el ejercicio de derechos, así como el cumplimiento de deberes a través de estos medios.

Desde la entrada en vigor en 2010 del anterior Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica hasta ahora, se han producido numerosos cambios en España en particular y en la Unión Europea en general, que han incrementado y transformado los procesos de transformación tecnológica y digital de una manera notoria. Dicha situación ha originado un nuevo escenario en materia de ciberseguridad, en el cual se ha evidenciado que los sistemas de ciberseguridad están cada vez más expuestos violaciones de seguridad, siendo prueba de ello el gran aumento de ciberataques que se ha venido produciendo, tanto en número como en sofisticación.

Bajo esta tesitura, el nuevo ENS, establece su aplicabilidad a:

- Los sistemas de información de todo el **sector público,** entendiendo por tal:
  - — La Administración General del Estado.
  - — Las Administraciones de las Comunidades Autónomas.
  - — Las Entidades que integran la Administración Local.
  - — El sector público institucional, es decir:
    - ■ Cualesquiera organismos públicos y entidades de derecho público vinculados o dependientes de las Administraciones Públicas.
    - ■ Las entidades de derecho privado vinculadas o dependientes de las Administraciones Públicas.
    - ■ Las Universidades públicas.
- Los sistemas de información de las entidades del **sector privado**, cuando, de acuerdo con la normativa aplicable y en virtud de una relación contractual, presten servicios o provean soluciones a las entidades del sector

público para el ejercicio por estas de sus competencias y potestades administrativas.

- Los sistemas que tratan información clasificada.

Por consiguiente, y en la medida en la que a determinadas entidades del sector privado les es de aplicación el ENS en lo que respecta a su relación con las entidades del sector público, **las entidades públicas españolas están obligadas a incluir en sus pliegos referencias al cumplimiento del Esquema Nacional de Seguridad**, concretamente, los pliegos de prescripciones administrativas o técnicas de los contratos que celebren las entidades del sector público incluidas en el ámbito de aplicación de este real decreto deben contemplar todos aquellos requisitos necesarios para asegurar la conformidad con el ENS de los sistemas de información en los que se sustenten los servicios prestados por los contratistas, tales como la presentación de las **correspondientes Declaraciones o Certificaciones de Conformidad con el ENS.**

Tal y como se pone de manifiesto en la Guía de Seguridad de las TIC CCN-STIC 809 Declaración, Certificación y Aprobación Provisional de conformidad con el ENS y Distintivos de cumplimiento[5]:

- Cuando se trate de sistemas **de categoría BÁSICA**, se trate dará publicidad a la conformidad de los sistemas de información afectados mediante una **Declaración de Conformidad**. La Declaración de Conformidad con el ENS podrá representarse mediante un Sello o Distintivo de Declaración de Conformidad,
- Cuando se trate de sistemas de **categorías MEDIA o ALTA**, el sistema de información deberá superar la correspondiente Auditoría, y se dará publicidad a la conformidad de los sistemas de información afectados mediante la exhibición de una **Certificación de Conformidad**.

Mediante la inclusión de referencias al Esquema Nacional de Seguridad en sus pliegos de condiciones, las entidades públicas pretenden garantizar que sus procesos de contratación se llevan a cabo de acuerdo con los requisitos de seguridad establecidos en el ENS, y que los proveedores que contratan cuentan con las medidas de seguridad adecuadas para proteger la información que manejan.

Importante destacar que las entidades a las que les es de aplicación el ENS tienen un plazo de dos años desde la entrada en vigor del nuevo ENS, esto es, hasta el 5 de mayo de 2024.

---

5 Guía de Seguridad de las TIC CCN-STIC 809 Declaración, Certificación y Aprobación Provisional de conformidad con el ENS y Distintivos de cumplimiento <https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/1279-ccn-stic-809-declaracion-de-conformidad-con-el-ens/file.html#:~:text=La%20Declaraci%C3%B3n%20de%20Conformidad%20con,qui%C3%A9n%20en%20esta%20hubiere%20delegado>

3. PRIVACIDAD DESDE EL DISEÑO Y POR DEFECTO. PRINCIPIOS FUNDAMENTALES

La privacidad desde el diseño (PdD) es un enfoque de la protección de datos que consiste en integrar desde el principio consideraciones de privacidad en el diseño de la tecnología y los procesos. El objetivo de la PdD es actuar de forma proactiva en el cumplimiento de la normativa, trayendo, desde el momento de la concepción del tratamiento, la normativa protectora de datos de carácter personal. Pensando en la privacidad y sus riesgos desde el origen, mitigarlos y así evitar tener que afrontar y enfrentar los efectos negativos que se producen a posteriori.

Se trata, por tanto, de un cambio en la concepción que tenemos a la hora de integrar los aspectos jurídicos-legales en la creación de proyectos en el seno de las entidades. **Es el punto de partida en cualquier hoja de ruta que se precie en materia de protección de datos de carácter personal.**

Ann Cavoukian[6] introdujo el concepto "Privacy by desing"[7][8] que, como hemos venido indicando, busca una relación win-win en los nuevos proyectos de sistemas de información en los que sean susceptibles de introducir datos de carácter personal.

Win-Win entre innovación y derechos fundamentales que se configura como un binomio indivisible al que hay que buscarle una relación de equilibrio. En el ciclo de vida de los sistemas de información se puede actuar de dos formas:

- Antes: actuar de forma proactiva respecto a la privacidad permitirá integrar ésta en el proceso de análisis y diseño, evitando costosas rectificaciones posteriores debido a no haberla tenido en cuenta.
- Después: se corre el riesgo de propiciar un rechazo por parte de los actuales y futuros clientes y/o usuarios, dañando de forma irremediable la imagen del sistema de información, o lo que es peor, de la entidad.

En consecuencia, el enfoque basado en la PbD aumenta la eficacia y la eficiencia del proyecto.

La legitimación de este concepto la encontramos en el artículo 25 del RGPD, en el que se indica expresamente: *1. Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento,*

---

6 Ann Cavoukian, Identity in the Information Society, Ago 2010, Volume 3, Issue 2, pp 247-251. Privacy by design: the definitive workshop. A foreword by Ann Cavoukian, Ph.D https://link.springer.com/content/pdf/10.1007%2Fs12394-010-0062-y.pdf

7 Peter Hustinx, European Data Protection Supervisor. Privacy by Design: Delivering the Promises, Madrid 2009 https://edps.europa.eu/sites/edp/files/publication/09-11-02_madrid_privacybydesign_en.pdf

8 Resolución de Privacidad desde el Diseño. 32ª Conferencia Internacional de Comisionados de Privacidad y Protección de Datos.Jerusalén (Israel) 27-29/10/2010 <https://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_resolutionon_privacybydesign_en.pdf>

así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, ***el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas,*** *como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados. 2.****El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales q****ue sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas. 3.Podrá utilizarse un mecanismo de certificación aprobado con arreglo al artículo 42 como elemento que acredite el cumplimiento de las obligaciones establecidas en los apartados 1 y 2 del presente artículo".*

La concepción de PbD[9] expuesta por Ann Cavoukian pivota sobre las siguientes características:

1. Proactivo no reactivo/ preventivo no correctivo

La privacidad por diseño se anticipa a los riesgos sobre los datos personales, identificándolos, evaluándolos y tratándolos mediante la evaluación de riesgos y la adopción de medidas encaminadas a evitar que se materia-

---

[9] European Data Protection Supervisor (EDPS). Opinion 5/2018 Preliminary Opinion on Privacy by design, May 2018 <https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf> *"'Privacy by Design' or 'Data Protection by Design'? For the purpose of this Opinion, we use the term "privacy by design" to designate the broad concept of technological measures for ensuring privacy as it has developed in the international debate over the last few decades. In contrast, we use the terms "data protectionby design" and "data protection by default" to designate the specific legal obligations established by Article 25 of the GDPR."*

European Union Agency for Cybersecurity (ENISA). Privacy and Data Protection by Design, from policy to engineering, Dic 2014 https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design/at_download/fullReport *"The term "Privacy by Design", or its variation "Data Protection by Design", has been coined as a development method for privacy-friendly systems and services, thereby going beyond mere technical solutions and addressing organisational procedures and business models as well".*

Information Commissioner's Office (ICO). Data protection by design and default. <https://ico.org.uk/for-organisations/guide-todata-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-designand-default/> *"This concept is not new. Previously known as 'privacy by design', it has always been part of data protection law. The key change with the GDPR is that it is now a legal requirement."*

licen durante la transición y operación del sistema de información o los servicios que soporta.

2. **Privacidad por defecto**

   Cualquier sistema ha de estar configurado de forma que por defecto otorgue una mayor protección a la privacidad de las personas.

3. **Privacidad embebida en el diseño**

   La protección de la privacidad ha de estar integrada en el sistema de información desde el momento en que se diseña, sin que ello disminuya su plena funcionalidad. No se trata de una opción que se añade a posteriori, sino que, al contrario, es uno de sus componentes integrales.

4. **Visibilidad y transparencia**

   La entidad que gestione el sistema de información que trate datos personales ha de estar sujeta a los "términos y condiciones" y "política de privacidad" informados desde un principio y no deberían modificarse sin el previo aviso, y en su caso consentimiento, de los usuarios afectados. También deberían estar sujeta a una verificación independiente.

5. **Seguridad extrema a externo**

   La protección de la información se ha de configurar desde el momento en que se recaban los datos y durante todo el ciclo de vida del servicio o del sistema de información que los trata, hasta que éste es retirado y los datos sean utilizados para un nuevo servicio o destruidos. En este último caso se garantizará también que se elimine de forma segura y confidencial, respetando los periodos de retención establecidos.

6. **Respeto por el individuo**

   El interés del individuo siempre ha de estar presente en el diseño de sistemas de información, por ejemplo, mediante previsión de medidas de seguridad, mensajes informativos, opciones favorables al usuario, privacidad por defecto, etc.

7. **Suma positiva**

   Funcionalidad y privacidad no son excluyentes, sino que ambas han de estar garantizadas e integradas en cualquier sistema desde la fase del diseño. Se debe pensar que los usuarios no usarán aquellos servicios o sistemas de información en los que no confían por lo que, a la larga desaparecerán.

4. EL ANÁLISIS DE RIESGOS EN PROTECCIÓN DE DATOS

Como hemos venido comentando, la gestión de riesgos es un aspecto importante del Reglamento General de Protección de Datos, que exige a las organizaciones adoptar las medidas adecuadas para garantizar la seguridad de los datos personales y minimizar el riesgo de violación de los datos.

Según el RGPD, la gestión de riesgos[10] se refiere al proceso de identificar y evaluar los riesgos asociados con el tratamiento de datos personales, y aplicar medidas para mitigar o eliminar esos riesgos. El RGPD requiere que las organizaciones adopten un enfoque basado en el riesgo para la protección de datos, lo que significa que deben tener en cuenta la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los riesgos y la gravedad del daño potencial a los derechos y libertades de las personas.

El RGPD exige que las organizaciones apliquen medidas técnicas y organizativas adecuadas para garantizar la seguridad de los datos personales, teniendo en cuenta el estado de la técnica, los costes de aplicación y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas. Además, el RGPD exige que las evaluaciones de riesgos estén documentadas, con el fin de demostrar el cumplimiento de la normativa.

En general, la gestión de riesgos es un componente crítico del cumplimiento del RGPD, y las organizaciones deben adoptar un enfoque proactivo de la evaluación y gestión de riesgos con el fin de proteger los derechos y libertades de las personas con respecto al tratamiento de sus datos personales.

La pregunta llegados a este punto es cómo se debe llevar a cabo una gestión del riesgo adecuada y conforme a la normativa, pues bien, la Agencia Española de Protección de Datos (en adelante, AEPD), en su documento *"Gestión de riesgos y evaluación de impacto en el tratamiento de datos personales"* publicado en 2017 proporciona orientaciones a las organizaciones sobre cómo llevar a cabo la gestión de riesgos y la evaluación de impacto en sus actividades de tratamiento de datos personales.

El documento ofrece, en primer lugar, una visión general de los principios y conceptos en los que se basa la gestión de riesgos y la evaluación de impacto, incluyendo la identificación de riesgos, el análisis de su impacto potencial y la aplicación de medidas para mitigar o eliminar dichos riesgos. Se hace especial hincapié en la importancia de llevar a cabo análisis de riesgo y evaluaciones de impacto periódicas, y de documentar los resultados de dichas evaluaciones para demostrar el cumplimiento con el RGPD y la LOPDGDD.

Sin detrimento de lo anterior, es importante tener en consideración que, en el sector público la determinación de las medidas de seguridad viene dada por el Esquema Nacional de Seguridad, tal y como se ha venido exponiendo, por lo que, será a través de la realización del análisis riesgos asociado al ENS, como se determinen las medidas que deban implantarse en caso de tratamiento de datos personales para evitar su pérdida, alteración o acceso no autorizado,

---

[10] Guía "Gestión del riesgo y evaluación de impacto en tratamientos de datos personales" de la Agencia Española de Protección de Datos: <https://www.aepd.es/es/documento/gestion-riesgo-y-evaluacion-impacto-en-tratamientos-datos-personales.pdf>

adaptando los criterios de determinación del riesgo en el tratamiento de los datos.

5. EVALUACIÓN DE IMPACTO EN PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

El RGPD incorpora una nueva obligación para los responsables de tratamiento: evaluar el impacto de las operaciones de tratamiento en la protección de datos.

El texto legal no define el proceso de las Evaluaciones de Impacto en Protección de Datos, pero sí indica que, la ejecución de las EIPD se tendrán que sustentar en metodologías o métodos sistemáticos, para que resulten objetivas, repetible, comparables y estén documentadas.

El Considerando 84 RGPD indica de forma expresa que: *"A fin de mejorar el cumplimiento del presente Reglamento en aquellos casos en los que sea probable que las operaciones de tratamiento entrañen un alto riesgo para los derechos y libertades de las personas físicas, debe incumbir al responsable del tratamiento la realización de una evaluación de impacto relativa a la protección de datos, que evalúe, en particular, el origen, la naturaleza, la particularidad y la gravedad de dicho riesgo. El resultado de la evaluación debe tenerse en cuenta cuando se decidan las medidas adecuadas que deban tomarse con el fin de demostrar que el tratamiento de los datos personales es conforme con el presente Reglamento. Si una evaluación de impacto relativa a la protección de datos muestra que las operaciones de tratamiento entrañan un alto riesgo que el responsable no puede mitigar con medidas adecuadas en términos de tecnología disponible y costes de aplicación, debe consultarse a la autoridad de control antes del tratamiento.*

Es importante en este punto tener claro qué es una EIPD, y es que la evaluación de impacto en la privacidad es una herramienta esencial para aplicar el principio de responsabilidad proactiva, y se podría interpretar que una EIPD es un análisis de riesgos enfocado a la privacidad, es decir, un estudio pormenorizado de las consecuencias sobre la privacidad que tendrían la posible materialización de escenarios de riesgo no previstos o no deseados. Este estudio no es la aplicación literal de una fórmula, sino la aplicación de la metodología que permita converger a un resultado.

Descrito de esta forma pareciera que hablar de Análisis de riesgos y de EIPD es exactamente lo mismo, pero la realidad es distinta, y es que, si bien todos los tratamientos requieren de la realización de un análisis de riesgos que determine las medidas de seguridad a implementar, no todos los tratamientos requieren una EIPD. Para determinar qué tratamientos lo requieren, es preciso realizar un análisis previo de cada tratamiento para **valorar si entraña un riesgo alto.**

En el desarrollo de la privacidad desde el diseño y por defecto que comentábamos anteriormente, los análisis de riesgos y las EIPD son elementos claves en

el cumplimiento de tales principios y es que ambas (análisis de riesgos y EIPD), deben realizarse antes de que se ejecute el tratamiento, salvo que el tratamiento existiese antes de la entrada en vigor del RGPD y no haya sufrido modificaciones en su esencia. En tal caso, se debería realizar un proceso de evaluación, para adaptar las medidas de seguridad si fuera necesario.

La ejecución de la EIPD corresponde al responsable del tratamiento con la colaboración activa del encargado (si aplica) y el asesoramiento y apoyo del Delegado de Protección de Datos si lo hubiese. La realización de una EIPD es una tarea ardua que puede necesitar de la participación de otras áreas o personas que por conocimiento específico pueden ser clave a la hora de asesorar los riesgos (personal de seguridad o de la oficina del CISO, ICT, asesoría jurídica, etc.)

La metodología que se aplique para la realización de la EIPD es totalmente libre, aunque existen muchos modelos a disposición de las entidades.

El artículo 35 del RGPD articula las EIPD y nos sirve de guía para determinar si se debe realizar una EIPD a un tratamiento en cuestión o no es necesario. En mi opinión, a diferencia de lo que pudiera pensarse, el orden práctico de este artículo no responde a su orden número, y es que, la experiencia ha ayudado a interpretar este artículo y, por tanto, las EIPD, en el siguiente orden:

1. **Art. 35.5 del RGPD. La autoridad de control publicará una lista de los tipos de tratamiento que no requieren evaluaciones de impacto relativas a la protección de datos**[11].

   Parece lógico pensar que, el primer paso para determinar si un tratamiento tiene la obligación de pasar por una EIPD es comprobar que éste no sea uno del tratamiento que excepciona la propia AEPD. De esta forma, si el tratamiento a realizar por parte del responsable o del encargado del tratamiento está ahí incluido, bastaría con realizar un análisis de riesgos y establecer las medidas de seguridad oportunas.

2. **Art. 35.4 del RGPD. La autoridad de control establecerá y publicará una lista de los tipos de operaciones de tratamiento que requieran una evaluación de impacto relativa a la protección de datos12.**

   El RGPD establece para las autoridades de control, en nuestro caso, la Agencia Española de Protección de Datos, la misma obligación tanto en negativo (art.35.5 del RGPD), como en positivo (art.35.4 del RGPD). Es decir, insta a que cuente con un listado de determinados tratamientos para los que es necesario llevar a cabo una EIPD por entender que el trata-

---

11 El listado de tratamientos en los que no es necesario realizar una evaluación de impacto de la Agencia Española de Protección de Datos: <https://www.aepd.es/sites/default/files/2019-12/ListasDPIA-35.5l.pdf >

12 El listado de tratamientos en los que es necesario realizar una evaluación de impacto de la Agencia Española de Protección de Datos: <https://www.aepd.es/es/documento/listas-dpia-es-35-4.pdf>

miento en sí mismo, ya sea por la tipología de datos, la tecnología o, entre otros, el contexto, supone un alto riesgo para los derechos y libertades de los afectados.

Si bien lo anterior, la AEPD matiza en su listado que será necesario realizar una EIPD en la mayoría de los casos en los que dicho tratamiento **cumpla con dos o más criterios de la lista expuesta**. Cuantos más criterios reúna el tratamiento en cuestión, mayor será el riesgo que entrañe dicho tratamiento y mayor será la certeza de la necesidad de realizar una EIPD.

3. **Art. 35.3 del RGPD. Sin detrimento de las listas indicadas en los puntos anteriores, el propio RGPD también establece en su propio articulado supuestos en los que es necesario llevar a cabo una EIPD.**

   El tercer nivel de comprobación para determinar la necesidad o no de realizar una EIPD lo encontramos en el art. 35.3 del RGPD, en el que, el propio RGPD tasa tres supuestos particulares en los que habría que realizar una EIPD, concretamente cuando el tratamiento:

   a) suponga una evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar;
   b) sea a gran escala de las categorías especiales de datos, o de los datos personales relativos a condenas e infracciones penales.
   c) sea observación sistemática a gran escala de una zona de acceso público.

4. **Art. 35.1 del RGPD. Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas**.

   Este último nivel, ubica al responsable ante la tesitura de saber si el tratamiento entra o no un "alto riesgo", ya que de ello depende la necesidad o no de realizar una EIPD. La forma más objetiva de conocer si se está ante un tratamiento de alto riesgo es habiendo realizado con carácter previo un análisis de riesgos, ya que si, de la realización del mismo, se determina que el riesgo intrínseco del tratamiento es "alto o muy alto", será necesario realizar una EIPD conforme los parámetros del RGPD.

Una vez determinado si el tratamiento en cuestión es objeto de una EIPD conforme alguno de los cuatro niveles previamente descritos, lo siguiente será realizar la EIPD. En este punto, como señalábamos al comienzo, no se cuenta con una metodología concreta, el RGPD se limita únicamente a indica que la evaluación deberá incluir como mínimo:

- una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento;
- una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad;
- una evaluación de los riesgos para los derechos y libertades de los interesados, y
- las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con RGPD, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas.

Hay que tener muy claro que el fin último de la EIPD es reducir el riesgo asociado de forma intrínseca a un tratamiento mediante la aplicación de medidas de seguridad, ahora bien, qué sucede en aquellos casos en los que, una vez realizada la EIPD, y establecidas las medidas de seguridad más apropiadas, el riesgo continúa siendo alto. En estos casos, el RGPD crea lo que podemos llamar un comodín, y es que, en el art. 36 del RGPD, se regula la consulta previa, indicando que: *"1.El responsable consultará a la autoridad de control antes de proceder al tratamiento* ***cuando una evaluación de impacto relativa a la protección de los datos en virtud del artículo 35 muestre que el tratamiento entrañaría un alto riesgo*** *si el responsable no toma medidas para para mitigarlo. 2. Cuando la autoridad de control considere que el tratamiento previsto a que se refiere el apartado 1 podría infringir el presente Reglamento, en particular cuando el responsable no haya identificado o mitigado suficientemente el riesgo****, la autoridad de control deberá, en un plazo de ocho semanas desde la solicitud de la consulta, asesorar por escrito al responsable****, y en su caso al encargado, y podrá utilizar cualquiera de sus poderes mencionados en el artículo 58. Dicho plazo podrá prorrogarse seis semanas, en función de la complejidad del tratamiento previsto. La autoridad de control informará al responsable y, en su caso, al encargado de tal prórroga en el plazo de un mes a partir de la recepción de la solicitud de consulta, indicando los motivos de la dilación. Estos plazos podrán suspenderse hasta que la autoridad de control haya obtenido la información solicitada a los fines de la consulta. 3. Cuando consulte a la autoridad de control con arreglo al apartado 1, el responsable del tratamiento le facilitará la información siguiente: a) en su caso, las responsabilidades respectivas del responsable, los corresponsables y los encargados implicados en el tratamiento, en particular en caso de tratamiento dentro de un grupo empresarial; b) los fines y medios del tratamiento previsto; c) las medidas y garantías establecidas para proteger los derechos y libertades de los interesados de conformidad con el presente Reglamento; d) en su caso, los datos de contacto del delegado de protección de datos; e) la evaluación de impacto relativa a la protección de datos establecida en el artículo 35, y f) cualquier otra información que solicite la autoridad de control"*

Con todo, la decisión de la AEPD se basaría fundamentalmente en:

- los fines y medios del tratamiento previsto
- las medidas y garantías establecidas
- la evaluación de impacto

De ahí la gran importancia de mantener un control detallado y actualizado de todos los movimientos y procesos relacionados con los tratamientos de datos. En especial con aquellos de alto riesgo. Hacer una buena EIPD y delimitar correctamente el tratamiento puede suponer toda la diferencia.

6. SEGURIDAD DE LOS DATOS PERSONALES: APLICACIÓN DE MEDIDAS TÉCNICAS Y ORGANIZATIVAS APROPIADAS.

Realizado el análisis de riesgos y, en su caso, la EIPD, el siguiente paso es implementar las medidas de seguridad adecuadas.

La directriz general que hace el RGPD remite aquellas medidas que se consideren necesarias y adecuadas que deberán tener la *"capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento"* (art. 32 del RGPD).

Si bien el RGPD no cuenta con un listado de medidas a implementar, no es menos cierto a lo largo de su articulado, así como en sus considerandos menciona explícitamente determinadas medidas como:

- La seudonimización.
- La minimización.
- El cifrado de datos.
- Políticas internas de protección de datos de carácter personal.
- Códigos de conducta.
- Mecanismos de certificación.
- Proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas.

Obviamente, como punto de partida estas medidas son adecuadas pero se alejan bastante de esa máxima de seguridad tanto organizativa como técnica que se dirime por todo el articulado del Reglamento General de Protección de Datos. Las autoridades de control en estos últimos años han tratado de dotar de mayor contenido a este aspecto indicando otras medidas de seguridad tales como:

Medidas de seguridad organizativa

- Análisis del GAP y desarrollo de un plan de acción.
- Revisión de los modelos existentes de cumplimiento y políticas de empresa.

- Proceso de nombramiento de DPO(s) y afectación de recursos (reestructuración organizativa).
- Plan de formación corporativa.
- Diseño del registro de tratamientos.
- Modelo de EIPD homogeneizado.
- Procedimiento de notificación de brechas de seguridad.
- Plan de revisión PDCA.

Medidas de seguridad técnica

- Considerando que ningún texto refleja la exhaustividad del antiguo Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, una de las medidas técnico-organizativas que deben acometerse es la definición de un catálogo de medidas de seguridad técnica que sirva de base para las EIPD y demás tratamientos de riesgo inferior.
- La adhesión a códigos de conducta o mecanismos de certificación aceleran mucho este proceso.
- La aplicación de las medidas de seguridad de la antigua Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (y su reglamento de desarrollo) son una posible solución, siempre y cuando el análisis de riesgo realizado sobre los tratamientos concluya que éstas son suficientes y adecuadas.

7. NOTIFICACIONES DE VIOLACIONES DE SEGURIDAD

Para cerrar esta visión sobre la protección de datos y la seguridad de la información, debemos introducirnos en las notificaciones de violaciones de seguridad. Para ello es importante saber que el RGPD define la «violación de la seguridad de los datos personales» como toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos, y es que, aún y cuando se hayan aplicado todas las medidas de seguridad derivadas del análisis de riesgos o, en su caso, de la EIPD, hay que tener claro que **la seguridad no es inexpugnable.**

La materialización de la destrucción, pérdida, alteración, comunicación o acceso no autorizados a datos personales se produce con cierta asiduidad y frecuencia, burlando todas las medidas de seguridad aplicadas por el responsable o el encargado del tratamiento. En estos supuestos, **el RGPD establece una obligación adicional al responsable, y es la de notificar que la violación se ha producido**.

Ahora bien, en la práctica qué se podrían considerar brechas o violaciones de seguridad: (i) la pérdida o robo de un dispositivo (smartphone, ordenador portátil, tablet, etc.); (ii) el acceso no autorizado a las bases de datos de una organización (incluso por su propio personal); (iii) el borrado accidental de ficheros que contengan datos de carácter personal; (iv) la fuga de información por un ataque en la red corporativa, o (v) la pérdida de documentación con información sensible.

La comunicación, según el RGPD, debe realizarse sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, de ahí lo transcendental que es contar con un protocolo o política de gestión de violaciones de seguridad.

Debe darse un proceso previo cuyo objetivo sea preparase técnica y organizativamente para afrontar con diligencia y eficacia en caso de producirse una violación de seguridad. En esta etapa se debe identificar a los agentes implicados en la gestión de la misma, el análisis de riesgos y/o evaluación de impacto en caso de que sean necesarias y la definición de los planes de respuesta a incidentes.

Tras ello, vendría la fase de detección e identificación, en dónde se debe concretar qué se considera violación de seguridad y las herramientas, mecanismos de detección o sistemas de alerta con los que el responsable va a contar, así como el análisis de la información que proporcionen dichas herramientas.

Una vez detectada e identificada la violación de seguridad, habría que analizarla y clasificarla, indicando:

- Tipo de amenaza: código dañino, intrusiones, fraude, etc. Se trata de una breve descripción del incidente en función de la información de la que se disponga.
- Contexto u origen de la amenaza: interna o externa.
- Categoría de seguridad de los sistemas y datos afectados.
- El perfil de los usuarios afectados.
- Número y tipología de los sistemas afectados.
- Impacto del incidente en la organización y en los derechos y libertades de los afectados.
- Requerimientos legales y regulatorios.
- Vector de ataque: ruta o medio por el que se ha materializado el incidente.

A menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas, la misma deberá ser comunicada a la autoridad de control. El responsable (o encargado) o el DPD deberán comunicar la incidencia a la mayor brevedad posible a:

- La Autoridad Competente salvo si, como se ha indicado, la violación no supone un riesgo para los derechos y libertades de los afectados.

- Los propios afectados cuando la violación de seguridad entrañe un alto riesgo para sus derechos o libertades.

La comunicación no será necesaria si el responsable puede demostrar que la violación de la seguridad no entraña un riesgo para los derechos y las libertades de los interesados. Es decir:

- Si el responsable ha adoptado medidas técnicas/organizativas apropiadas antes de la violación de seguridad (i.e. el cifrado de la información, que hace ininteligibles los datos para terceros no autorizados).
- Si el responsable ha tomado las medidas correctivas que aseguren que ya no hay posibilidad de que el alto riesgo se materialice.
- Si la notificación a los interesados supone un esfuerzo desproporcionado. En este caso la comunicación pública de la violación de seguridad es una alternativa.

El informe de la violación debe ser completo y contener además las conclusiones de los técnicos y responsables del equipo. Elementos como una descripción objetiva del hecho, el protocolo de actuación seguido durante el evento, los elementos de seguridad existentes antes del incidente y aquellos que se han instalado después, etc. Son elementos clave para documentar convenientemente el incidente y procurar que no se repita.

El cierre del incidente se produce una vez que se han ejecutado las medidas de contención, se ha solucionado la violación de seguridad identificada y se ha recuperado el estado anterior a la producción del incidente.